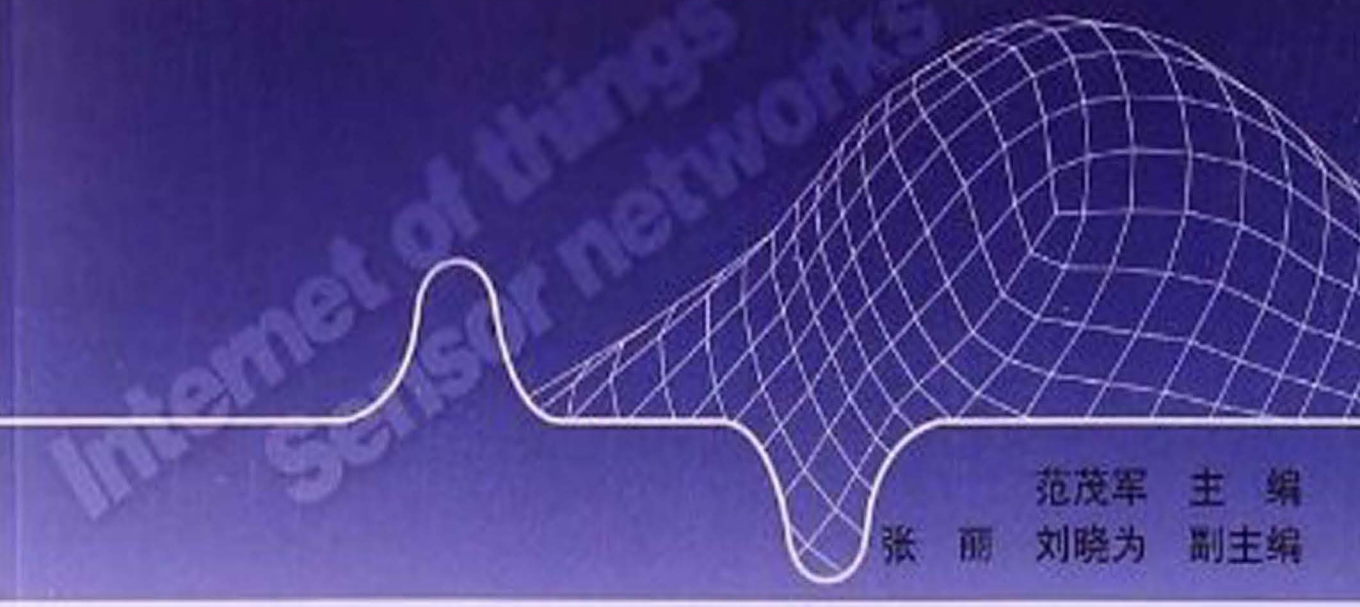
物联网与传感网工程实践



范茂军 主编
张 丽 刘晓为 副主编

★ 以直观与感性为着手点，让读者认识到物联网即物流与电子信息流融为一体的有针对性的服务网络

★ 主要内容涉及物联网技术的基本原理、系统组成、关键技术、典型案例等

★ 由业内多名专家精心打造，化繁为简，集专业知识与实践内容于一体

★ 专业类入门书籍，为读者解决工程实际问题奠定一定的基础

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

物联网与传感网工程实践

范茂军　　主　编

张　丽　刘晓为　副主编

卜雄珠　付敬奇　孙为民　于梅芳　丁　群

施云波　段成丽　周晓宁　齐久成　高鹏麟　参　编

雷　垒　李明云　张新忠　唐　洁　王勃然

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

为了给物联网的参与者和初涉信息技术应用的年轻工程师们提供一个较为简单的系统知识结构和专业技术构成的入门类书籍，本书把基本知识和应用实践案例等联系在一起，主要内容包括物联网应用技术，物联网中物体的标记、定位与时间同步，物体信息传输网络与要素控制，物体特征数据的传输与路由，物联网与传感网中故障诊断、容错、修复与安全，无线传感网的设计与测评，传感网与物联网的服务管理与应用等。

本书适用于物联网的参与者和初涉信息技术应用的工程师们，以及对物联网感兴趣的读者，也可作为高等院校物联网工程专业以及电气信息类专业的本科生、研究生教材和教学参考用书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

物联网与传感网工程实践/范茂军主编. —北京：电子工业出版社，2013.3

ISBN 978-7-121-19819-9

I. ①物… II. ①范… III. ①互联网络－应用 ②智能技术－应用 ③无线网 IV. ①TP393.4 ②TP18 ③TN92

中国版本图书馆 CIP 数据核字（2013）第 048387 号

策划编辑：李 洁
责任编辑：李 洁 齐 岳
印 刷：北河市鑫马印装有限公司
装 订：北河市鑫马印装有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：18.5 字数：408.8 千字
印 次：2013 年 3 月第 1 次印刷
印 数：4 000 册 定价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

PREFACE

物联网是新一代信息技术的重要组成部分，对于许多非专业人员很难用简单的语言表述它是什么样的技术。为了使读者，尤其是初学者，尽快掌握其内涵及在工程中的实现方法，本书从直观的感性知识角度入手，让读者认识到物联网就是物流和电子信息流融为一体的有针对性的服务网络。也可以简单地说，实现这样的信息服务网络主要解决四个问题：人与物、人对人、物对物之间的信息交流，以及各种需求的配送与交换。现有的各种网络技术体系更多地体现了服务和信息交流，这就是现阶段的物联网。

对于学习物联网技术的人们来说，只有了解它的基本原理、系统组成、关键技术、典型案例等问题，才能较全面地掌握其系统知识。为帮助非电子信息类的毕业生、工作不久的工程师及非电子信息类的成熟工程师了解物联网的基本理论和工程实现所涉及的基本技术。本书用了较大篇幅讲解了物联网工程实现中所涉及的基本理论、概念。中间部分介绍了传感网、物联网技术和面对应用的服务等技术。从对象之间的时间、空间关系出发，根据人们对物联网的要求，将人与人、物与物、物与人之间的联络和服务联系在一起。从人们在任何时间、地点的各种需求都能被及时满足的角度出发，将各种需求与现有的技术和网络相结合。从互联网、物流网、远程教学、远程医疗、网上购物、网上交友等信息技术现实的应用等方面，让人们感受到物联网技术已融入到我们的生活之中。

在物联网中，随着新技术的不断加入，工程实现中必须考虑将许多新的软件和硬件更新到应用终端中，以满足用户对服务不断增长的需求。如果站在服务与被服务的角度来看，物联网所涉及的信息技术除了经典的三大关键技术，即信息采集——传感器技术、信息传输——有线无线通信及网络技术、信息处理——计算机与信息处理技术外，更多的是信息处理方面的内容和面向对象的服务。

从技术层面来看，这种服务的网络，面对各种需求引发的信息，其数据量几乎以每年一倍的速度增长。在硬件方面，全球生产的的存储器几乎都用到了这类商业服务之中；在软件方面，随着这种快速增长的需要，各种应用工具和管理软件应运而生。计算机走向了超大存储，大数据提出了云计算，这些都是在物联网概念产生之前就已经孕育出来的。再

如应用中的软件问题：大数据处理和服务带来的应用和技术问题；服务中的软硬件结合的问题；大数据存储、分发与路由，分布式存储与信息处理等问题。今天人们常用的分布式处理和嵌入式技术、中间件到“云计算”为解决大数据的处理与信息汇聚提供了技术发展的支持；网络与通信中的有线无线传输，使电信运营商变成物联网的网络层；传感器与信息采集系统，成为传感网和感知层。尤其在感知的概念下，传感器和传感网更成为人们热议的话题。

从服务信息交换过程看，首先要获得对象的相关信息，通过传感器和汇聚结点组成的传感网，将信息传送到公共网络上，再由公共的网络——通信和网络，进行远距离传送、分发、交换，最后将众多的信息传送到信息处理中心——计算机，由计算机进行计算处理，物联网的服务商再将这些信息汇聚、存储、分类、归并，按用户的需要，分发传送给各个用户，为他们提供所需的各种信息服务。服务是物联网的最大特点，人们随时就能直接体会到谷歌、百度、维基解密等网站提供的信息服务，享受到物流公司提供的将在线购买的产品送到客户手中的服务，以及其他可通过网络实现的各种服务。而且，很多服务网站甚至可以跟踪我们的生活习惯，将我们每天上网观看的信息整理汇总、分析，当我们再次输入自己关心的词汇时，网站就会马上提供给我们相关的内容和链接。物联网的应用就在人们身边，并且相关技术还会不断进步与发展。

物联网是电子信息技术的应用，它会为人们提供所需要的数据和信息。利用档案技术建立日志、目录的方法，可以实现对所有信息的建档和检索。利用无线传感网和移动互联网技术实现的物联网信息服务技术，使网络应用从原来的信息资源由网络拥有者提供，变为网络信息资源可由使用者和拥有者共同提供，这就是物联网的技术特点之一。现在，人们只要将需要的服务和内容的关键词输入到搜索引擎中，各种信息就可被检索到。如果需要深度服务，可将它们汇聚一起，再通过后台的服务器及软件，筛选出人们所需要的内容。

随着物联网应用规模的扩大，数据存储、处理与服务必然会遇到大数据问题。大量用户同时使用，必然会出现因数据流量引起的冲突并发等问题。因篇幅限制，本书对此只做了简要的介绍，相关内容可参考更专业的书籍。最常见的数据汇聚方法，就是利用爬虫工具将想搜索的各种信息，通过引擎和对象特征在网上的数据和信息，“爬”到需要的资源数据库中。通过分类、排序为用户及时提供来自各方的信息，并完成数据的汇聚和提炼。

物联网中有关数据创造、连接和更新等问题，如对物体的语音与图像识别等，都是建立在传感和数据处理之上，通过统计与运算的技术方法实现的。物联网应用系统所涉及的技术，多是现有的电子技术，其产品形态就是现有的和正在开发的电子产品。现阶段具有代表性的产品就是智能手机，它就是物联网系统中的多功能终端的一种典型代表。

在物联网工程实践中，初学者能够尽快掌握主要技术是关键。本书编者多是来自教学和工程实践一线的专家、教授和工程师。在他们的精心提炼下，将分散复杂的相关知识归

纳成 7 个章节来向读者介绍。由于各校的教学重点不同，专业目标不同，教师可根据各自的教学计划有选择地进行讲解。

对于学生和初学者来说，可从应用实践案例等入手，从繁杂无序的独立概念中解脱出来，认清物联网是一种应用技术的本质。掌握信息领域中的三大关键技术，在工作中根据各自工作对象的实际情况正确地选择相关的技术和产品，灵活准确地实现各自独特的任务要求，是成为一名具有解决工程问题能力的合格工程师的关键。

本书第 1 章介绍了互联网和传感网的概念和技术，在 2、3 章分别介绍了物体定位与标识的方法和物体信息传输网络与要素控制。第 4 至 6 章主要介绍了数据生成、传送、分发、故障分析等相关技术，并介绍了无线传感网的设计与测评。第 7 章介绍了物联网应用的信息服务及管理的问题，并介绍了相关的典型应用案例。在硬件方面，由于涉及内容繁多，本书只对在物联网应用中较独特的部分如定位和标识传感器、二维条码、RFID、MEMS 和微传感器等作简单的介绍，对已经广泛使用的多种传感器不再赘述，更多的内容请读者参考传感器类相关书籍。

本书由中国电子科技集团公司第三研究所范茂军研究员担任主编，南京理工大学张丽教授和哈尔滨工业大学刘晓为教授担任副主编。参加编写的还有南京理工大学卜雄珠教授，上海大学付敬奇教授，哈尔滨工程大学孙为民教授，南京邮电大学于梅芳教授，黑龙江大学丁群教授，哈尔滨理工大学施云波教授，总装备部电子元器件合同管理办公室段成丽参谋，中国酒泉卫星发射中心周晓宁高工，中国白城兵器实验中心齐久成高工，工信部电子工业标准化研究院高鹏麟高工，航天科工集团雷垒，北京瑞普光电有限公司李明云总经理，黑龙江联通公司张新忠高工，南京理工大学唐洁博士、新西兰奥克兰大学王勃然博士。特别对为本书出版辛勤工作的电子工业出版社徐静、李洁两位编辑，以及为本书提供相关案例和工程素材的同志，在此一并表示感谢。

范茂军

2013 年 3 月

目 录 CONTENTS

第 1 章 物联网应用技术概论 …… 1

1.1 物联网、传感网与互联网基本概述 …… 1
1.1.1 物联网 …… 2
1.1.2 传感网 …… 3
1.1.3 互联网、传感网与物联网 …… 5
1.1.4 网络接入与管理 …… 5
1.2 物联网与相关技术标准 …… 7
1.2.1 ITU-T 物联网标准 …… 8
1.2.2 ETSI 物联网标准 …… 10
1.2.3 3GPP/3GPP2 物联网标准 …… 10
1.2.4 IEEE 物联网标准 …… 11
1.2.5 中国物联网标准 …… 12
1.3 应用技术系统与物联网技术构架 …… 13
1.4 物体的标识与定位 …… 15
1.5 物体状态与特性的识别 …… 16
1.5.1 物联网中的信息获取与管理 …… 16
1.5.2 传感器 …… 17
1.5.3 性能评价与选用原则 …… 19
1.6 智能传感器与嵌入式系统 …… 22
1.6.1 智能传感器 …… 22
1.6.2 嵌入式系统 …… 24
1.7 微传感器及 MEMS 技术 …… 25
1.8 并行处理与云计算 …… 29

第 2 章 物联网中物体的标识、定位与时间同步 …… 31

2.1 条码技术 …… 31
2.1.1 一维条码技术 …… 31
2.1.2 二维条码技术 …… 34
2.2 RFID 技术 …… 37
2.2.1 RFID 的原理及特性 …… 37
2.2.2 RFID 的组成 …… 40
2.2.3 RFID 工作频率与分类 …… 47
2.2.4 RFID 中间件 …… 49
2.2.5 RFID 与条码的比较 …… 55
2.2.6 RFID 系统设计中的注意事项 …… 57
2.2.7 射频技术典型应用 …… 59
2.2.8 RFID 遇到的挑战 …… 60
2.3 中间件 …… 61
2.3.1 中间件分类 …… 61
2.3.2 中间件基本结构 …… 64
2.3.3 中间件的设计原则 …… 68
2.3.4 中间件设计目标与功能实现 …… 71
2.3.5 设计平台 …… 75
2.4 无线测距定位技术 …… 77
2.4.1 结点间测距的基本方法 …… 78
2.4.2 计算结点位置的基本方法 …… 79
2.4.3 定位算法的分类 …… 82
2.4.4 定位算法的性能评价 …… 84
2.5 其他无线测距定位技术 …… 85
2.6 典型卫星定位系统 …… 87
2.7 物体间时间同步机制与方法 …… 89
2.8 时间同步协议 …… 95
2.8.1 基于 Receiver-Receiver（接收方—接收方）机制的时间同步协议 …… 95

2.8.2 基于成对机制的时间同步协议 ····· 96
2.8.3 基于 Sender-Receiver（发送—接收方）机制的时间同步协议 ····· 99
2.8.4 典型时间同步协议的比较 ····· 100

第 3 章 物体信息传输网络与要素控制 ····· 101

3.1 有线与无线网络的选择 ····· 101
3.1.1 无线网络的基本概念 ····· 101
3.1.2 无线局域网与协议 ····· 102
3.2 网络频率分配 ····· 106
3.2.1 频率分配的核心内容 ····· 106
3.2.2 频率分配的数学模型 ····· 109
3.3 网络中的信道分配 ····· 110
3.4 结点的功率与功耗分配 ····· 111
3.4.1 功率分配的作用 ····· 111
3.4.2 功率分配对系统的影响 ····· 112
3.4.3 典型的功率控制协议与算法 ····· 114
3.5 接口技术与标准 ····· 115
3.5.1 SCSI 小型计算机系统接口 ····· 115
3.5.2 USB ····· 118
3.5.3 SATA 接口 ····· 122
3.5.4 IDE 电子集成驱动器 ····· 123
3.6 结构与散热设计 ····· 123
3.6.1 电子产品结构设计的一般要求与原则 ····· 123
3.6.2 电子产品的结构设计过程 ·· 124
3.6.3 散热设计 ····· 125

第 4 章 物体特征数据的传输与路由 ····· 127

4.1 数据中心式路由 ····· 127
4.1.1 数据中心式路由协议 ····· 127
4.1.2 以数据为中心的路由机制缺陷分析 ····· 131
4.2 集群结构式的路由 ····· 133
4.2.1 集群技术的组织形式 ····· 133
4.2.2 集群技术的交换结构 ····· 134
4.2.3 集群路由器 ····· 135
4.2.4 集群路由器分类 ····· 136
4.2.5 集群路由器的优点 ····· 139
4.3 位置信息路由 ····· 140
4.3.1 位置服务协议 ····· 141
4.3.2 几种典型的位置路由算法 ····· 145
4.4 无线传输路由与常用协议 ····· 151
4.4.1 表驱动路由协议 ····· 151
4.4.2 源发起按需路由 ····· 154
4.5 ZigBee、Wi-Fi 与蓝牙技术 ····· 157
4.5.1 ZigBee ····· 157
4.5.2 Wi-Fi ····· 172
4.5.3 蓝牙技术 ····· 186

第 5 章 物联网与传感网中故障诊断、容错、修复与安全 ····· 195

5.1 物联网与传感网常见故障类别 ····· 195
5.1.1 传感器网络故障原因 ····· 195
5.1.2 传感器网络故障分类 ····· 196
5.2 物联网与传感网常见故障诊断 ····· 197
5.2.1 故障诊断目的及性能标准 ··· 197
5.2.2 故障诊断技术 ····· 199
5.2.3 传感器故障诊断技术 ····· 199
5.2.4 传感器网络故障诊断技术 ····· 201
5.2.5 无线传感器网络与传统 IP 网络故障诊断区别 ····· 201
5.3 物联网与传感网常见纠错与修复 ···· 202
5.3.1 物联网与传感网故障修复的特点 ····· 202

5.3.2 几种常见的威胁分析与对策 …… 203
5.4 结点与组件安全 …… 205
5.4.1 物联网和传感网的特点 …… 205
5.4.2 WSN 网络结点安全 …… 205
5.4.3 密钥管理机制 …… 206
5.4.4 网络结点的能耗问题和节能技术 …… 207
5.5 无线传感网安全 …… 207
5.5.1 无线传感器网络安全问题分析 …… 207
5.5.2 无线传感网安全要求 …… 208
5.5.3 无线传感网安全问题 …… 208
5.6 加密技术 …… 212
5.6.1 密钥 …… 212
5.6.2 数据加密的实现 …… 216
5.6.3 加密技术的应用 …… 217
第 6 章 无线传感网的设计与测评 …… 219
6.1 WSN 协议框架设计 …… 219
6.2 WSN 路由设计 …… 228
6.2.1 WSN 路由协议的特点 …… 228
6.2.2 无线传感器网络路由协议的要求 …… 230
6.2.3 无线传感器网络路由协议的分类 …… 231
6.3 WSN 协议测评 …… 232
6.4 WSN 协议试运行与验收 ……238
6.5 典型系统应用案例 ……243
第 7 章 传感网与物联网的服务、管理与应用 ……246
7.1 传感网服务质量与评价原则 ……246
7.1.1 服务质量 ……246
7.1.2 无线传感网的服务质量 ……251
7.1.3 服务质量保障 ……253
7.2 传感网管理 ……257
7.3 传感网常用的操作系统 ……261
7.3.1 无线传感器网络特点及其对操作系统的特殊需求 ……261
7.3.2 TinyOS 开放源代码操作系统 ……262
7.4 传感网系统设计与分析 ……264
7.5 典型系统设计与应用案例 ……265
7.5.1 在 ETC 系统中的应用……265
7.5.2 在水环境监测中的应用 ……267
7.5.3 在家庭监护中的应用 ……269
7.5.4 在商城中的应用 ……269
7.5.5 在机场安全系统中的应用 ……277
7.5.6 在电网故障诊断中的应用 …278
7.5.7 在制造系统中的应用 ……279
7.5.8 在工业中的应用 ……280
7.5.9 在远程医疗中的应用 ……282

第 1 章　物联网应用技术概论

1.1　物联网、传感网与互联网基本概述

从哲学角度来观察社会科学和自然科学以及经济和技术发展的关系，我们不难看出：尽管物联网、传感网、互联网具有鲜明的专业技术和应用技术特征，属于自然科学中信息领域研究范畴的问题，但它们的发展和演变遵守着各自的发展道路和共同的发展规律。如果把它们放到社会经济发展的背景下来观察，就很容易发现很多技术和概念，其产生和演变都和特定的历史背景和经济发展有着明显的对应关系。回顾物联网、传感网、互联网这三个名词的产生也具有鲜明的社会发展历史特色，与其他名词和概念一样，脱离不了全球经济与技术发展的历史痕迹。从各自的技术核心和特征来看，物联网从功能上是在互联网、传感网等概念上衍生出来的一种满足人们更多需求的一种应用网络；从电子信息技术角度来说，是计算机、网络与传感器技术及软件的综合技术。它是将各种物品与网络结合在一起，满足人们各种需要的应用技术。其基本的方法是，将各种传感器通过用户端延伸扩展到各种物品之间，使物品通过传感器和计算机及网络和服务系统联系成一体，形成一个可以满足人们各种需求的信息交换网络。

美国 MIT 的 Kevin 提出物联网概念时，就想采用 RFID（射频识别）和各种传感器将各种物品联系到一起为人们的生产和生活服务。后来国际电信联盟 ITU 的研究报告描述了物联网相关的内容和知识，即把所有可能的物体都加上传感器，通过传感器获取物体的自身状态、周围的环境状态，通过物联网将所有可能的信息全部融入其中。

在欧洲，业内人士认为物联网在空间上应是物理和虚拟的实体集合；在实体范畴它应是在时间和空间上可移动的、可标识的、可进行信息交换的。

在国内，目前一般认为物联网是使任何一个物体的信息相互联系，使人们的需求和愿望得到更高更新的满足，通过这个新的物联网技术来带动科学、生产和社会的发展。

因此，物联网技术的发展不仅需要更多的科技工作者参与，更需要从事相关工作的工程师和物联网应用的管理者的参与。本书力图从理论组成、技术结构、软硬件性能到典型工程案例等，叙述其技术构成、应用方法和相关标准，使读者能结合已有知识比对出体系和特点，从而正确把握其实质，并在实践中不但完善丰富其内涵。本项技术也不例外，它也是在已有的多项技术上，针对人们不断的需求设计出的新名词。物联网技术从原始概念的提出，至今已有十多年的历史，也在被不断地完善和丰富。因此，在科学技术飞速发展的今天，它也像众多新生技术一样，被需求和新技术不断地丰富和完善，已经越来越不像最初的定义。而人们正是在这种不断演变中，不断提炼其内涵，扩展其外延，这才推动了各种技术的发展和进步。

为了使读者在阅读本书后也能快速理解相关的技术内容，本书中一些专用技术名词也直接采用了英语名词，这样将方便与同类资料的链接和融通。

1.1.1 物联网

物联网概念最早是由美国麻省理工学院 Auto-ID 研究中心提出的，其基本思想是：为物体之间实现联系，并能够区分出所有物体之间的不同，采用先对物体进行标记，再用传感器将所采集到的各种信息传到互联网上，使得所有物体的各种信息联系到在一起，通过计算机处理需求和资源之间的供求关系，及时配置可能满足需求者的各种需要。物联网从技术架构层次上来看，人们习惯按功能将它分为三层：感知层、网络层和应用层。从物联网基础技术来看，它主要包括两方面内容：一方面是互联网技术，在此技术基础上扩展网络应用，延伸到所有可能的物体和物体之间的信息交换和通信；另一方面是传感器技术，将所有物品通过相应的传感器和 RFID 等，将感知的各种信息变成可以识别的电信号。

国际电信联盟在《The Internet of Things》2005 年报告中对物联网概念进行扩展，提出物联网是在任何时刻，任何地点，任意物体之间实现的互联。各类对象之间的基本关系如图 1-1 所示。

在欧洲，2008 年的《Internet of Things in 2020》报告中指出：未来物联网发展 RFID 和对物体识别的传感器技术是未来物联网的基石。由于标识和信息提取是物联网技术的关键，致使后来人们更加关心 RFID 和传感器等在信息采集、标识等技术在物联网的应用。紧接着欧盟于 2009 年 9 月 15 日发布了《Internet of Things Strategic Research Roadmap》研究报告，明确要求在欧洲不同 RFID 和物联网项目之间的组合，以及协调包括 RFID 的物联网研究的活动。

在亚洲，日韩之后，我国也开展了此方面的研究，在经历高热之后人们看到物联网更像互联网和传感器结合的应用。一方面，由于网络技术快速的成熟，需要新的动力激发更多的人关注并创造出新的概念，引导信息技术和市场的发展。另一方面，由于早期人们认

为物联网是未来互联网的一个组成部分，并从网络技术角度来评价物联网时，希望它成为基于标准的并可互操作的通信协议，有能力实现资源动态的全球配置的网络基础架构。

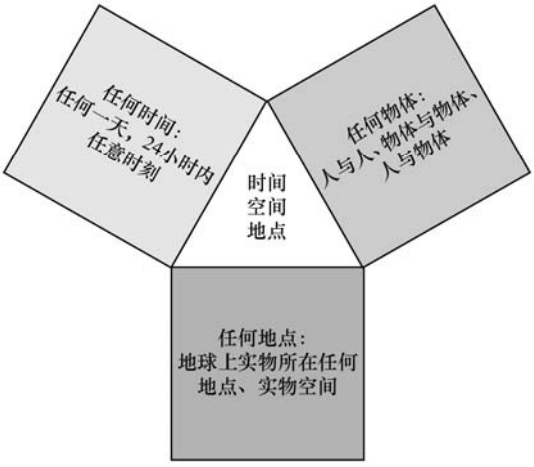


图 1-1　物联网中的时间、空间和物体之间的关系

物联网技术所涉及的内容较广，除网络、智能终端、传感器技术等，还涉及很多软、硬件技术和应用。在现今技术条件下，如用户可获得各种智能接口与社会环境进行连接和通信，就有可能使被标识过的物体满足人们的需要。为了解决对人们要求的问题，通常采用计算机构成一个虚拟的电子信息空间，对掌握的各种资源和需求进行设计和分配，来满足人们精神和物质的需求。

1.1.2　传感网

“传感器网络”承担着对自然界各种信息数据采集汇总的主要任务，而互联网络是传递到达各端点的载体。在实际应用中，二者通常是联合使用，是实现物与物、物与人、人与人之间信息交互、提供信息服务的智能网络信息系统。

“无线传感网”是由若干具有无线通信功能的传感器结点构成的网络。这种网络最早是由美国国防部高级研究计划局（DARPA）在 1978 年提出的，并资助了卡耐基－梅隆大学开展了分布式传感器网络技术的研究。用户、对象、信息交换等各单元和网络之间的关系，国外认为传感网的基本结构与特点如图 1-2 所示。

随着研究的深入，人们开始想到未来的网络会深入到人们生活的每个角落，可为人们提供各种可能的服务。而这些服务终端的信息离不开各种各样的传感器，人们在原研究的基础上又提出了泛在的传感器网络（USN）的概念。这种传感网络的特点，首先是网络结点由具有通信及智能化的传感器结点组成；其次在任何时间、地点，任何物体的周边都布

置有这种功能的传感网络。这样的传感网络可为各种需求提供相应的服务，从环境监测到安全保卫，从生产到生活，提供无所不能的服务。

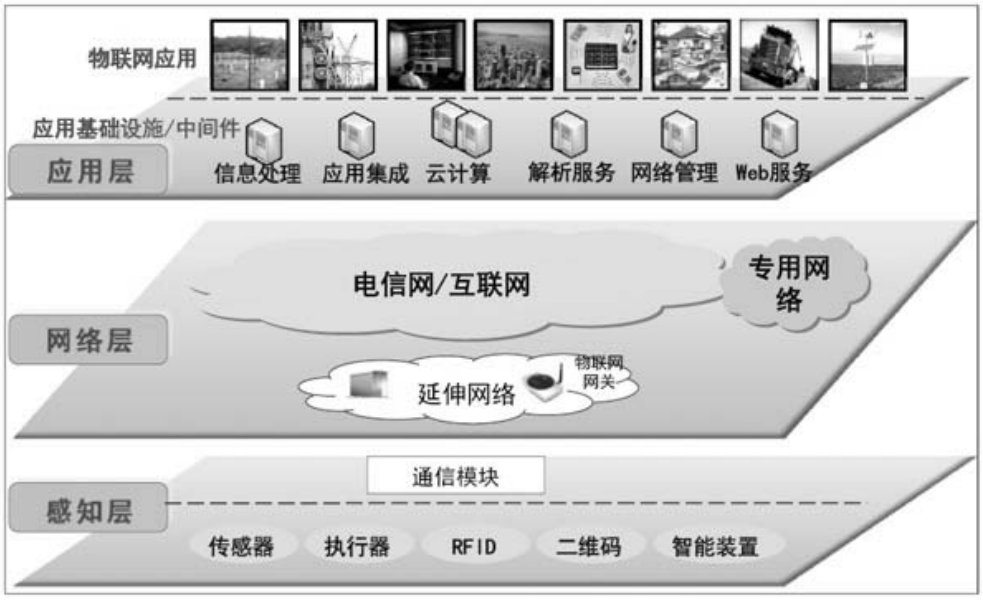


图 1-2　用户终端、对象现场、信息处理、网络分发与传递、传感器的联网

“泛在网”概念最早是由日韩提出。它们认为，无所不在的网络社会将是由智能网络、最先进的计算技术以及其他领先的数字技术基础设施组成的技术社会形态。根据这样的构想，USN 网络将以无所不在、无所不包、无所不能为基本特征，帮助用户实现任何时间、任何地点、任何人、任何物都能顺畅地通信。其底层是由各种传感器、执行器、RFID 等各种信息设备组成，负责对物理世界的感知与反馈。

国际电信联盟在 2008 年年初的研究报告中，阐述了泛在传感器网络体系的基本架构。并指出泛在传感网自下而上的基本结构是：传感器网络、泛在传感器网络接入网络、泛在传感器网络基础骨干网络、泛在传感网的中间件、泛在传感网应用平台五个层次。

泛在传感器网络接入网络是实现底层传感器网络与上层基础骨干网络的连接，由网关、sink 结点等组成；泛在传感网的基网有 Internet、下一代网络（NGN）；泛在传感网中间件处理、存储传感数据，并以服务的形式提供对各类传感数据的访问；泛在传感网是实现各类传感网应用的技术支撑平台。

目前我国信标委所属的传感器网络标准工作组认为，传感器网络具体表现在它综合了微型传感器、分布式信号处理、无线通信网络和嵌入式计算等多种先进信息技术，能对物理客体进行信息采集、传输和处理，并将处理结果以服务的形式发布给用户。

1.1.3　互联网、传感网与物联网

目前人们对人与物、物与物广泛互联、实现人与客观世界的全面信息交互的网络的命名，一直存在着物联网、传感网、互联网这三个称谓。回顾其发展历史，可从这些概念归纳后得出一个基本一致的结论。这些概念间的关系，如图 1-3 所示。

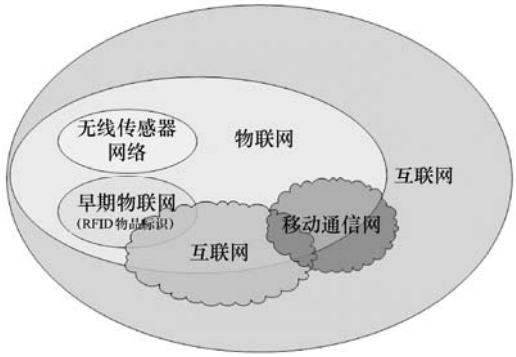


图 1-3　互联网、传感网、物联网等之间的关系

在传感网的概念中，如果将传感器的概念进行扩展，认为 RFID、二维条码等信息的读取设备和音视频录入设备等数据采集设备都是一种特殊的传感器，则范围扩展后的传感器网络即简称为与物联网概念并列的“传感网”。而从 ITU-T、ISO/IEC JTC1/SC6 等国际标准组织对传感器网络、物联网定义和标准化范围来看，传感器网络和物联网其实是一个概念、两种不同的表述，其实质都是依托于各种信息设备实现了物理世界和信息世界的无缝融合。此外，在业界也有观点认为，物联网是从产业和应用角度，传感网是从技术角度，对同一事物的不同表述，但其实质是完全相同的。因此，无论从哪个角度，都可以认为目前为人所熟知的“物联网”和“传感网”这两个概念，都是以传感器、RFID 等客观世界标识、感知技术，借助于无线网络、互联网、移动网等通信网络实现人与物理世界的信息交互。而泛在网是面向泛在应用的各种异构网络的集合，且更强调跨网之间的信息融合与应用。

1.1.4　网络接入与管理

物联网技术是各方面的信息相互交互和服务的新型网络，其主要解决的是相关网络的接入和管理。

（1）无线传感器网

无线传感器网是物联网重要的基础技术，在结构上它是由各种传感器结点组成的。这种网络的特点是多跳的自组织网，当采用适当的协议也可使无线通信网络和有线网络相连接。

在网络的管理方面，不仅要有灵活的路由机制，而且支持多种类型设备的协同工作。信息采集是各种各样的无线传感器，在技术方面还包括各种可即插即用、低功耗、低成本的智能传感器和无线网技术支持的 WSN 无线传感器网络等。

（2）移动网与网络接入

移动网：是目前覆盖最广、应用最多的网络。采用无线终端接入设备最普及、最有效的接入手段。在技术上要针对人与人通信的需要，强化人和物之间的通信，以及物与物之间的通信能力。开发好各种设备的接入技术，接入利用好现有的各种网络设备，是推广物联网应用的有效方法。

网络接入：移动通信技术是目前解决有限产地和环境的物与物、人与物之间的沟通的主要手段。这种异构网络接入效率的主要措施有：增强 L2/L3 协议，支持大量低数据率终端的接入；简化同步、小区搜索、随机接入、切换过程以及移动性管理；采用更低带宽、更低码率编码的传输方式，支持更小资源的分配；简化调度、功控、HARQ 和链路自适应等问题。

（3）网络与终端管理技术

在网络与终端管理中，由于各种设备的接入标准不同（如 LAN、Wi-Fi、WiMaX、GSM、TD-SCDMA、WSN 等），为使各类异构网络能够实现互联互通，必须选择相对统一的标准接入方式。因为在这种由多种设备组成的异构网络中，还必须能支持各终端或网元间的相互协同以及临时的动态组网等，这样才能提高物与物、物与人之间的互联效率。

为了避免物联网中各类用户汇聚在一起时造成拥塞，对网络的管理显得十分重要。只有通过管理，提高畅通的信道和纯净的质量，才能使各种设备、网络终端获得预期的功效。更多的后端管理技术和服务，是支持大量终端的多种接入方式的重要措施。

（4）信息处理与能耗管理

信息处理是物联网应用中的主要技术问题，也是保证系统高效运行的重要因素，当传感器将采集到的信息汇聚到业务平台时，信息处理平台要对接收到的各种信息进行存储、处理、分析和数据挖掘后，才能为用户提供所需要的服务。在对这些信息进行处理时，需要利用更好更新的计算方法（如云计算、模糊识别等）来解决海量信息处理的问题。这样才能实现网内不同地域、不同用户对信息和数据进行处理分析的要求。

能耗是物联网应用中的重要技术问题，因为在有限的电能源的条件下，尤其在无线网络中各结点及系统携带的能量有限的情况下，对于能耗的管理与系统的信息管理一样重要，而在众多的信息进入整体网络时，这个问题更显得重要。常会出现多个用户同时在各自终端上操作，中央机也同时进行着大量的运算，以便优化决策和配置。此时网中需要消耗大量的能源，是常态下的数倍至百倍以上。在有限能源情况下，尤其是有的只能依靠自备电池或能量转化技术来工作，必须对系统能耗的各种问题进行细致思考。

对传感网来说，不仅要考虑其网络优化的问题，也要考虑能耗问题。在无线传感器网络（WSN）中，结点成本、功耗和体积等技术问题，是走向普及的重要问题，随着微电机系统（MEMS）、低功耗无线通信协议和数字电路的发展，改变了传感网传统的设计思想。传统的设计是将物理的基础设施和 IT 基础设施分开，如一方面是机场、公路、建筑物，另一方面是数据中心、网络、手机、个人计算机等。而现在已经开始将钢筋混凝土、电缆与芯片、网络等的设计和施工等方面结合到一起来进行。在此意义上，基础设施更像是一块新的地球工地，世界的运转就在它上面进行，其中包括经济管理、生产运行、社会管理乃至个人生活。物联网将引发新的“聚合服务”。

（5）开发环境与安全技术

高效、快捷的开发应用是物联网应用的重要问题。良好的应用开发环境，能够使应用软件相对独立于计算机硬件和操作系统平台。采用分布式计算是常用的一种重要措施，这不仅能满足数据量大，运算速度快的要求，而且可提高操作系统的能力。物联网的许多终端处于无人环境中，由于感知结点组群化、终端结点数量巨大、移动性低等特点，必须要求各种终端的安全性。其基本要求包括：防火、防盗、通信安全、存储安全、终端使用环境安全等，必须具有较高性能稳定性和可靠性。

1.2　物联网与相关技术标准

在标准方面，与物联网相关的标准化组织较多。物联网涉及极为广泛的技术种类，包括总体构架、传感技术、通信网络技术、应用技术等很多方面。很多标准组织从不同的角度对物联网进行研究工作，比如从机器到机器通信（M2M）的角度，从泛在网的角度，从互联网的角度，或从传感网和传感技术的角度，有的则关注于总体架构，等等。目前介入物联网领域的标准组织主要有 IEEE、ISO、ETSI、ITU-T、3GPP、3GPP2 等，下面我们会一一做介绍。

国际电信联盟（ITU-T）及欧洲电信标准化协会（ETSI）M2M 技术委员会主要从总体架构方面对物联网进行研究，两者研究的角度不同：ITU-T 从泛在网角度研究，而 ETSI 则从 M2M 的角度来研究总体架构。

国际标准化组织（ISO）、美国电气及电子工程师学会（IEEE）则专注于研究传感技术和器件方面的标准，主要涉及无线传感网。

第三代合作伙伴计划（The 3rd Generation Partnership Project，3GPP）和第三代合作伙伴计划 2（3rd Generation Partnership Project 2，3GPP2）主要研究物联网所应用到的通信网络技术，只限定在移动网络层面。

总的来说，目前为止，物联网的唯一标准在国际上尚未建立，已有的各标准组织自成体系，标准内容涉及架构、通信、传感、编码、数据处理、应用等多方面。

与传统的计算机和通信领域的标准体系有很大不同（传统的计算机和通信领域标准体系一般不涉及具体的应用标准）的是，物联网相关的标准组织都比较重视应用方面的标准制定。在电子检测、家居智能化、交通运输、电子消费应用等领域都有相当数量的标准正在制定中，这也说明了“由应用主导物联网”的观点在国际上已经达成了共识。

图 1-4 是不同领域的物联网相关主要标准组织的分布情况。本节选择一些在物联网领域重要的有一定影响力的标准组织进行介绍。

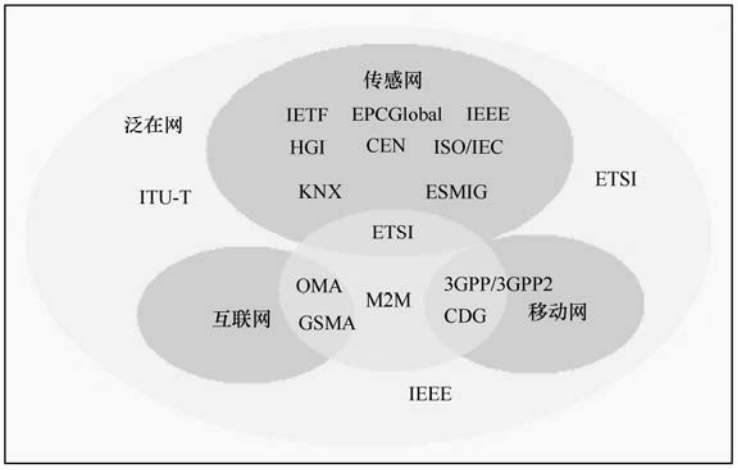


图 1-4　物联网在不同领域的主要标准组织分布情况

1.2.1　ITU-T 物联网标准

国际电信联盟远程通信标准化组织（ITU-T for ITU Telecommunication Standardization Sector），它是国际电信联盟管理下的专门制定远程通信相关国际标准的组织。国际电联作为世界最为普遍认可的信息通信标准制定者的角色，可以追溯到机构的创立之初。国际电联自 1865 年成立以来，一直在为行业的技术与服务达成共识而奔走，因为它们构成了世界上规模最大且互联最为紧密的人为体系的中坚力量。仅 2007 年，国际电联电信标准化部门（ITU-T）就制定了 160 多项新的和经修订的标准（ITU-T 建议书），涵盖了从核心网络功能与宽带到 IPTV 等下一代业务的各个方面。ITU-T 早在 2005 就开始进行泛在网的研究，可以说是最早进行物联网研究的标准组织。

ITU-T 主要研究泛在网总体框架、标识及应用方面。ITU-T 在泛在网研究方面已经从需求阶段逐渐进入到框架研究阶段，目前研究的框架模型还处在高层层面。图 1-5 为 ITU-T

提出的物联网架构。在标识研究方面，ITU-T 与 ISO 进行合作，关注于基于对象标识（OID）的解析体系；在健康和交通运输方面 ITU-T 也展开了研究。

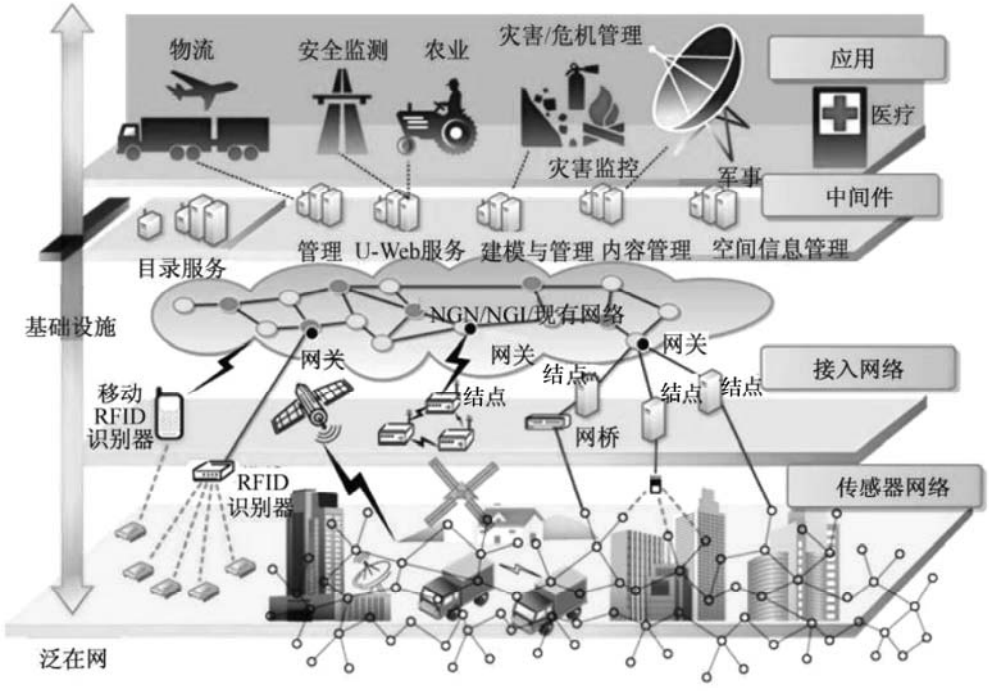


图 1-5　ITU-T 提出的物联网架构

ITU-T 相关研究课题组的研究情况如下。

SG13 主要从 NGN（Next Generation Network，下一代网络，又称为次世代网络）角度进行泛在网络相关的标准研究，韩国是标准研究的主导国家。目前标准化工作集中在基于泛在网络/无线传感器网络的需求和框架方面，支持标签应用和结构框架的研究，身份管理（IDM），还包括 NGN 的车载通信支持方面的研究等。

SG16 专门成立了一个小组进行泛在网络应用的研究，日、韩是研究共同主导，研究内容侧重于业务和应用，标识解析等方面。SG16 组研究的具体内容包括：Q.25/16 泛在传感器网络（USN）的应用和服务，Q.27/16 通信/智能交通系统（ITS）服务/应用的网关平台，Q.28/16 电子健康的多媒体框架，Q.21 和 Q.22 标记研究（主要是提出了标识应用需求和架构）。

SG17 设立了一个特别的问题小组展开泛在网络安全、身份管理的分析研究。SG17 组研究的具体内容包括：Q.6/17 泛在网络的通信安全，Q.10/17 身份管理框架和机制，Q.12/17 抽象语法标识（ASN.1）、OID 及相关注册。

SG11 成立了一个特殊的问题小组专门研究“NID 和 USN 测试规范”，主要研究结点标识（NID）和泛在传感器网络（USN）的测试构架，以及 H.IRP 和 X.oid-re 测试规范。

ITU-T 还在智能家居、车辆管理等应用方面开展了一些研究工作。

1.2.2 ETSI 物联网标准

欧洲电信标准化协会（European Telecommunications Standards Institute，ETSI）是由欧共体委员会 1988 年批准建立的一个非营利性的电信标准化组织，总部设在法国南部的尼斯。ETSI 的标准化领域主要是电信业，并涉及与其他组织合作的信息及广播技术领域。ETSI 作为一个被 CEN（欧洲标准化协会）和 CEPT（欧洲邮电主管部门会议）认可的电信标准协会，其制定的推荐性标准常被欧共体作为欧洲法规的技术基础而采用并被要求执行。

ETSI 采用 M2M 的概念进行总体架构方面的研究，相关工作的进展非常迅速，是在物联网总体架构方面研究得比较深入和系统的标准组织，也是目前在总体架构方面最有影响力的标准组织。

ETSI 成立了一个特别小组（M2M TC），从 M2M 的视角进行相关标准的研究。ETSI 成立这样一个小组主要是因为：目前为止尽管存在很多 M2M 相关标准，涉及多种无线接口、格状网络、路由和标识机制等，但这些标准主要是针对一个特定的应用场景，是相互独立的，如何找出已有的相对分散的技术和标准中的不足，所做的工作却很少。在这样的研究背景下，相关的技术小组的主要研究对象是从端到端的全景视角研究机器对机器通信，并与相关技术的研究进行合作研究工作。

M2M TC 组的工作是：从利益相关者的收集和发展 M2M 的业务需要出发，建立一个端到端的高层体系结构，找出已有标准不能满足需求的地方并制定新的具体标准，将现有的组件或子系统映射到高层体系构架中，并解决方案之间的互操作性（测试标准）、硬件接口标准化以及与其他标准组织进行沟通与合作。

1.2.3 3GPP/3GPP2 物联网标准

The 3rd Generation Partnership Project（3GPP）是领先的 3G 技术规范机构，是由欧洲的 ETSI，日本的 ARIB 和 TTC，韩国的 TTA 以及美国的 T1 在 1998 年年底发起成立的，旨在研究制定并推广基于演进的 GSM 核心网络的 3G 标准，即 WCDMA、TD-SCDMA、EDGE 等。中国无线通信标准组（CWTS）于 1999 年加入 3GPP。

3GPP 和 3GPP2 也从 M2M 的角度进行标准研究。作为移动网络技术的主要标准组织，3GPP 和 3GPP2 侧重于互联网网络能力的提高，是网络层相关方面研究的主要标准组织。

3GPP 的研究主要从移动网络出发，研究 M2M 应用对网络的影响，包括网络优化技术。它的主要研究领域包括：移动网络的 M2M 通信；定义 M2M 服务，而不包括具体的 M2M

应用的定义。Verizon、Vodafone 和其他的许多移动运营商在 M2M 的应用中发现了很多问题，如大量 M2M 终端对网络的冲击，系统控制能力不足等。因此，在高通、Vodafone、Verizon、三星等公司的推动下，3GPP 加速了 M2M 的研究，基本完成了需求分析、网络体系结构和技术框架研究，但核心的无线接入网络（RAN）的研究还没有开展。

相比之下，3GPP2 的相关性研究进展较慢。

1.2.4　IEEE 物联网标准

美国电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）是 1963 年 1 月 1 日由美国无线电工程师协会（IRE，创立于 1912 年）和美国电气工程师协会（AIEE，创建于 1884 年）合并而成，它是一个区域和技术互为补充的组织结构，以地理位置或者技术中心作为组织单位（如 IEEE 费城分会和 IEEE 计算机协会）。它管理着推荐规则和执行计划的分散组织（如 IEEE-USA 明确服务于美国的成员、专业人士和公众）。总部设在美国纽约。IEEE 在 150 多个国家中拥有 300 多个地方分会。透过多元化的会员，该组织在太空、计算机、电信、生物医学、电力及消费性电子产品等领域中都是主要的权威。专业上，它有 35 个专业学会和两个联合会。IEEE 发表多种杂志、学报、书籍和每年组织 300 多次专业会议。IEEE 定义的标准在工业界有极大的影响。在物联网的感知层研究领域，IEEE 的重要地位显然是毫无争议的。目前无线传感网领域用得比较多的 ZigBee 技术就基于 IEEE 802.15.4 标准。

IEEE 802 系列标准是 IEEE 802 局域网/城域网标准委员会制定的 LAN/MAN 技术标准。IEEE 802.15 工作组成立于 1998 年，专门从事无线个人局域网络（WPAN）的标准化工作。在 IEEE 802.15 工作组内有 5 个工作组，分别制定适合不同应用的标准。这些标准的传输速度，功耗和支持服务等方面都存在差异。

TG1 工作组制定 IEEE 802.15.1 标准，即蓝牙无线通信标准。该标准适用于移动电话，掌上计算机和其他设备中的中、短距离通信。

TG2 工作组制定 IEEE 802.15.2 标准。

TG3 工作组制定 IEEE 802.15.3 标准，研究超宽带（UWB）标准。本标准适用于网络多媒体中的高速、短距离通信中的应用。

TG4 工作组制定 IEEE 802.15.4 标准，研究低速率无线个人局域网（WPAN）。该标准力图实现低能耗，低比特率传输和低成本，专为个人或家庭在不同的设备之间提供了一个统一的标准低速网络标准。

TG5 工作组制定 IEEE 802.15.5 标准，研究无线个人局域网（WPAN）的无线网状网络（MESH）。该标准的目的是研究 MESH 组网的个人局域网的物理层和链路层的必要机制。

传感器网络的特点与低速率无线个人局域网（WPAN）有很多相似之处，因此，传感

器网络的物理层和媒体访问控制层（MAC）是基于 IEEE 802.15.4 标准的，其中最著名的是 ZigBee。因此，IEEE 802.15 工作组也是物联网领域的无线传感器网络的一个主要标准组织之一。我国也参与了一系列 IEEE 802.15 标准的开展工作，包括 IEEE 802.15.4c 和 IEEE 802.15.4e 的起草工作等。IEEE 802.15.4c 扩展了适合我国使用的频段，IEEE 802.15.4e 则扩展了工业级控制部分。

1.2.5 中国物联网标准

总的来说，我国物联网标准的制定工作还处于起步阶段，但发展迅速。目前我国已有涉及物联网总体架构、无线传感网、物联网应用层面的众多标准正在制定中，并且有相当一部分的标准项目已在相关国际标准组织立项。我国研究物联网的标准组织主要有传感器网络标准工作组（WGSN）和中国通信标准化协会（CCSA）。

WGSN 是由中国国家标准化管理委员会批准筹建，中国信息技术标准化技术委员会批准成立并领导，从事传感器网络（简称传感网）标准化工作的全国性技术组织。WGSN 于 2009 年 9 月正式成立，由中国科学院上海微系统与信息技术研究所任组长单位，中国电子技术标准化研究所任秘书处单位，成员单位包括中国三大运营商、主要科研院校、主流设备厂商等。传感器网络标准工作组将“适应中国社会主义市场经济建设的需要，促进中国传感器网络的技术研究和产业化的迅速发展，加快开展标准化工作，认真研究国际标准和国际上的先进标准，积极参与国际标准化工作，并把中国和国际标准化工作结合起来，加速传感网标准的修订工作，建立和不断完善传感网标准化体系，进一步提高中国传感网技术水平”作为其宗旨。目前 WGSN 已有一些标准正在制定中，并代表中国积极参加 ISO、IEEE 等国际标准组织的标准制定工作。由于成立时间尚短，目前 WGSN 还没有形成可发布的标准文稿。

CCSA 于 2002 年 12 月 18 日在北京正式成立。协会的主要任务是为提供更好的通信标准开展研究工作，将通信企业、制造企业、研究机构、大学和其他有关的企业和机构组织起来，按照公平、公正、公开的原则制定标准，对标准进行的协调和控制，并把高技术、高水平、高质量的标准推荐给政府机关等，将具有中国自主知识产权的标准推向世界。2009 年 11 月，CCSA 建立了一个新的泛在网络技术委员会（TC10），开展具体的物联网相关研究工作。虽然 TC10 刚成立不久，但在之前 CCSA 对物联网上的相关领域也做了一些研究。目前，CCSA 有多个与网络相关的标准正在制定，但没有发布。

在 2009 年 4 月成立的 RFID 标准工作组也是与物联网相关的标准研究组织。该工作组在工信部的领导下，开展科学和技术工作，致力于中国的 RFID 技术领域的标准研究和制定工作，取得了一定的成绩。

RFID 和 CCSA 标准组织都独立开展工作，每一组织的研究工作各有侧重。WGSN 侧

重于传感器网络，CCSA TC10 强调网络通信和应用研究，RFID 标准工作组则关注 RFID 相关领域。同时，标准工作组的研究领域也有很多交集，如 WGSN 也涉及传感器网络的通信部分和应用部分内容，CCSA 也涉及一些传感器网络方面的工作内容。对于这些交集领域，每一个标准之间必须保持良好的横向沟通与协调，基于此目的，国家正在筹备成立“网络标准联合工作组”。联合工作组旨在整合中国物联网相关标准资源，共同发展网络技术研究，积极推进物联网的标准化工作，加快发展物联网技术标准的步伐，需要政府部门对物联网产业发展决策提供全面的技术支持和服务支持。

1.3　应用技术系统与物联网技术构架

在实际工程中，当对象明确后就可构架出物联网的应用系统。最基本的应用系统包括物品命名管理系统、物品身份真伪验证系统、物联网系统管理等，特定应用系统包括仓储管理系统、楼宇监控系统、环境监测系统等。

物联网应用系统需要区分物联网端和互联网端。通常物联网端部署在有源 CPS 结点上，可以作为应用系统的客户端（客户机/服务器），也可作为应用系统的对等端应用模式（P2P，Peer-to-Peer，对等）。应用系统互联网端部署在互联网 CPS 结点上，可以作为应用系统的服务器端（客户机/服务器），也可以作为应用系统的 P2P 应用模式，但都需要提供较为强大的存储和后端处理能力，满足物联网应用需求。

目前国内外普遍认为物联网是一项综合性的技术，是一个服务和应用系统，没有哪家公司可以全面独立完成物联网的整个系统规划和建设。理论研究方面各行各业都在展开，而实际应用很少能跨出行业。物联网的规划和设计与推广发展是物联网技术生命的关键，运用好现有的器件（RFID、传感器）和软件（嵌入式软件）以及传输数据计算等资源是推动物联网技术的普及和用发展的核心。物联网构成主要有三个步骤：

1）对物体属性进行标识，属性包括静态和动态的属性，静态属性可以直接存储在标签中，动态属性需要先由传感器实时探测。

2）需要识别设备完成对物体属性的读取，并将信息转换为适合网络传输的数据格式。

3）将物体信息通过网络传输到信息处理中心（可能是分布式中心，如家里的计算机或者手机，也可能是集中式的，如中国移动的 IDC），由处理中心完成物体通信的相关计算。

在国内物联网应用案例中，具有代表性的案例是：上海浦东国际机场防入侵与世博会安防系统、苏州高铁物联网、济南园博园路灯控制系统、清华易程公司票务系统等。

上海浦东国际机场防入侵系统铺设了 3 万多个传感结点，覆盖了地面、栅栏和低空探测，可以防止用户的翻越、偷渡、恐怖袭击等攻击性入侵；济南园博园采用 ZigBee 技术的

路灯控制系统，是无线技术的路灯照明节能环保技术的应用典型，园区所有的功能性照明都采用了 ZigBee 无线技术达成的无线路灯控制；国内首家高铁物联网技术应用中心为高铁物联网产业发展提供科技支撑。以往购票、检票的单调方式，将在这里升级为人性化、多样化的新体验。刷卡购票、手机购票、电话购票等新技术的集成使用，让旅客可以摆脱拥挤的车站购票；与地铁类似的检票方式，则可实现持有不同票据旅客的快速通行。

智能交通系统（ITS 的应用），更是将通信、计算机、自动控制、传感器技术融合到一起，实现对交通的实时控制与指挥管理。在这个物联网系统中，交通运营信息的采集，为交通控制和交通违章管理等提供了基本的保证。

从以上物联网的几个典型应用系统可以看出，人们通常把物联网的技术架构按照功能分为三层：感知层、网络层和应用层。这三层的结构体系关系如图 1-6 所示。

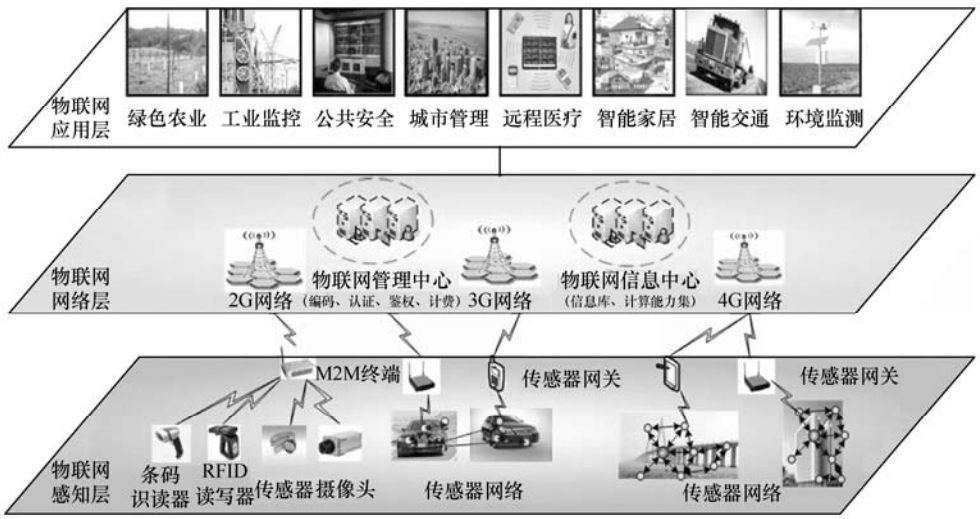


图 1-6　物联网三层结构和基本功能

感知层：主要功能是感知和识别物体，采集并捕获信息。产品的形式有二维码标签和识读器、RFID 标签和读写器、摄像头、GPS、各种传感器、传感器结点组成的自治网络、M2M（Machine to Machine）终端和传感器网关等，实现“全面感知”。

网络层：是指普遍的通信网络和服务的基础设施，包括各种通信网络与互联网形成的融合网络，还包括物联网管理中心、信息中心、云计算支撑平台、专家系统等对海量信息进行智能处理的部分。网络层不但要具备网络运营的能力，还要提升信息运营的能力，实现可靠的传送、交互和共享。

应用层：是将物联网技术与行业专业技术相结合，实现广泛智能化应用的解决方案集。利用云计算、模糊识别等各种智能计算技术，对海量的跨地域、跨行业、跨部门的数据和

信息进行分析处理，提升对物理世界、经济社会各种活动和变化的洞察力，实现智能化的决策和控制。

在物联网构架中，感知层是实现对物体信息及标识的感知，传感器是一种基本的嵌入设备。将来物体不仅自己专有各种基本的传感器，可以感知周围的各种信息，也可在有限的范围内相互感知。如在人进来房屋后，室内的灯自动打开，人离开之后灯会自动关闭。在智能家居环境中，基本设施中配有 Wi-Fi、WiMAX、蜂窝网络等，各种设备可以随时接入到互联网上，人们可随时享受到互联网、传感网、物联网的服务。

1.4　物体的标识与定位

标识是对物体基本特征信息的标注。对整体对象而言，如一个汽车部件有轮胎、转向盘，不同的厂家有不同的标识。在这个标识里面，一种是这类的标识，另一种是具体物件的类标识。就像条码一样，排在前面的信息是类，后面的是具体产品。标识也需有层次结构，一个物体有很多的标识，标识之间怎样映射，标识和服务之间怎样映射，标识之间怎样兼容，是需要认真研究的内容。

物联网的特点是基于互联网的平台，能够查询全球范围内每一件物品信息的网络平台，物联网的索引就是 EPC 代码。产品电子代码“EPC”是目前对物品进行标记的主要方法。它的特点是强调适用于对每一件物品都进行编码的通用的编码方案，这种编码方案仅仅涉及对物品的标识，不涉及物品的任何特性。每一件物品的 EPC 代码在物联网中所起的作用就是相当于一个索引。很多概念并不是有了物联网概念后才有的，如 EPC 概念能付诸实施，靠的是最底层的 RFID 系统。EPC 系统的基本组成在硬件方面，包括电子标签和阅读器。

EPC 是一个代码，选择射频识别的方式作为一种载体。EPC 标签就是一种电子标签，也称为射频标签。通过物联网会产生巨大的社会效益和经济效益，任何东西都在物联网上，每个物品都有唯一的 EPC 代码，这样就可以通过物联网查到其档案情况，防伪等一系列问题也都可以得到了解决。这样看来物联网的概念和技术也是由众多已有的概念和技术合成的代名词。

RFID 技术发展的历史已有很长时间，它为物联网技术的发展奠定了良好的基础。如将 EPC 标签（RFID）放到一本书上，当这本书通过阅读器时，阅读器则将 EPC 标签里面的信息采集到系统中。因阅读器和计算机网络是连接起来的，通过中间件连到物联网系统，存入 EPCIS 服务器中。

射频识别技术是一项利用射频信号通过空间耦合（交变磁场或电磁场）实现无接触资

讯传递并通过所传递的资讯达到识别目的的技术。通常由电子标签（射频标签）和阅读器组成。电子标签记忆体有一定格式的电子数据，常以此作为待识别物品的标识性资讯。应用中将电子标签附着在待识别物品上，作为待识别物品的电子标记。阅读器与电子标签可按约定的通信协议互传资讯，通常的情况是由阅读器向电子标签发送命令，电子标签根据收到的阅读器的命令，将记忆体的标识性数据回传给阅读器。这种通信是在无接触方式下，利用交变磁场或电磁场的空间耦合及射频信号调制与解调技术实现的。有关电子标签的内容将在第 2 章中进行详细的介绍，这里不再赘述。

物联网中的物和物之间的沟通标准，如人类的语言，如用同一种语言就可以在任何地点都不会产生语言障碍。EPC 并不是摒弃当前的标准，而是充分考虑如何将当前应用的编码方法与标准整合进去。如同从一维条码到二维码到射频技术的发展中，各种读写器的使用使各种信息可远距离地进行规范和统一的操作，实现信息的共享和交流。

物联网中的定位技术，是物品针对性服务的基本要素。3G 技术可进一步提高卫星定位的服务，使现有的系统很容易达到 10m 以内的定位精度，为城市内的人员、车辆、导航定位，以及高精度的紧急救护等提供更好的服务。常用的服务有：移动多媒体会议电话、会议电视服务。3G 网络高带宽的优点使得移动多媒体会议电话、会议电视服务由原来只能由专用网络提供，变成通过 3G 公用移动通信网络向中、小企业提供。企业管理者可以在旅途或车上，使用便携式计算机或其他 3G 终端设备（如移动 PDA），通过 3G 网络访问企业网络，处理业务问题，利用 3G 手机、移动 PDA 查询交通状况，接收大型会议定制的用户服务，为运动会、演唱会、展览会定制的服务，以及电台、电视台、报纸等公众媒体提供的移动阅读服务。

1.5 物体状态与特性的识别

1.5.1 物联网中的信息获取与管理

传感网是物联网的重要技术支撑，它是由各种传感器组成的信息获取的网络，是物联网感知和获取信息的主要手段。作为物联网中获取信息的感知层，是物联网的最底层，它与其他两层的关系如图 1-7 所示，图中椭圆虚线内为通常所说的感知层。其功能是完成对相关信息的采集、转换和收集。中间层为传输层，主要完成有线和无线的入网的接入，实现信息的分发与传送；最上一层为应用层，是将收集到的各种信息处理后，由应用平台控制指令发送到控制器，供用户使用。故通常称为应用层。

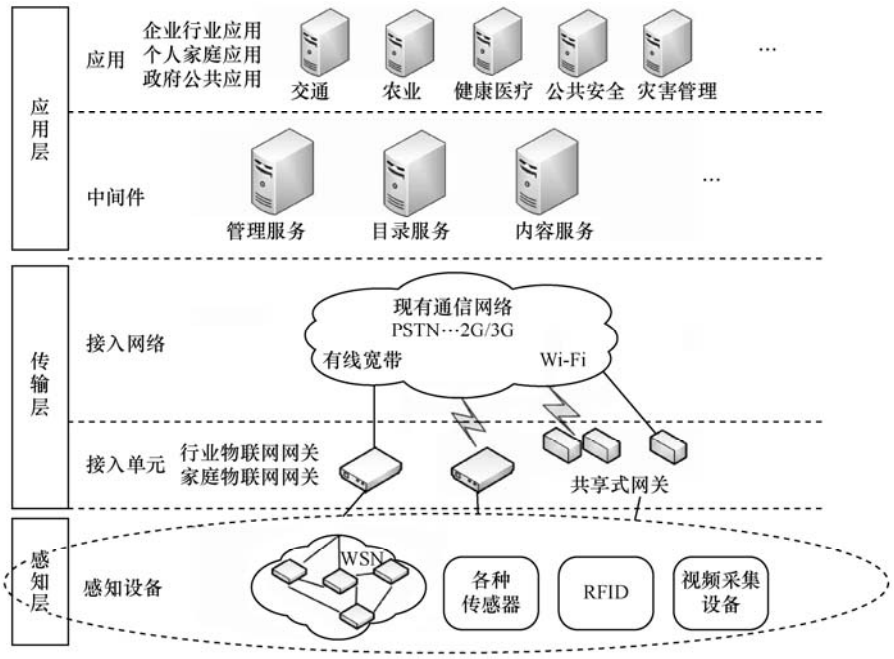


图 1-7　物联网构架和相关的网络和硬件之间的关系

1.5.2　传感器

传感器是一种能把被测量信息按一定规律转换成某种可用信号输出的器件或装置，以满足信息的传输、处理、记录、显示和控制等要求。应当指出，这里所谓的“可用信号”是指便于处理、传输的信号，一般为电信号，如电压、电流、电阻、电容、频率等。社会进步到今天，人们周围使用着各种各样的传感器：电冰箱、微波炉、空调机有温度传感器；电视机有红外传感器；录像机和摄像机有湿度传感器、光传感器；液化气灶有气体传感器；汽车有速度、压力、湿度、流量、氧气等多种传感器，这些传感器的共同特点是利用各种物理、化学、生物效应等实现对被检测量的测量。可见，在传感器中包含着两个必不可少的概念：一是检测信号；二是能把检测的信息变换成一种与被测量有确定函数关系的而且便于传输和处理的量。例如，传声器（话筒）就是这种传感器，它感受声音的强弱，并转换成相应的电信号；气体传感器感受空气环境中气体浓度的变化；电感式位移传感器能感受位移量的变化，并把它们转换成相应的电信号。传感器的一般分类方法如图 1-8 所示。

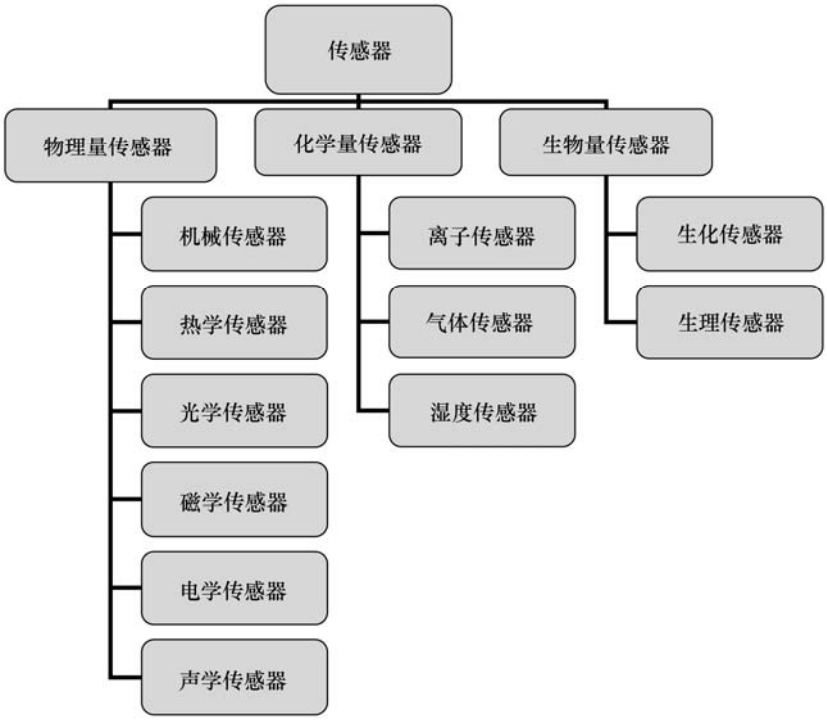


图 1-8　传感器的一般分类方法

在国家标准 GB/T 7665—1987《传感器通用术语》中，传感器被定义为：“能感受规定的被测量并按照一定的规律转换成可用信号的器件或装置，通常由敏感元件和转换元件组成。其中，敏感元件是指传感器中能直接感受或响应被测量的部分；转换元件是指传感器中将敏感元件感受或响应的被测量转换成适于传输或测量的电信号部分。”原机械工业部在其制定的《过程检测控制仪表术语》中对传感器的定义是：“借助于检测元件接收物理量形式的信息，并按一定规律将它转换成同样或别种物理量形式的信息仪表。”《新韦氏大词典》中的定义是：“传感器是从一个系统接收功率，通常以另一种形式将功率送到第二个系统中的器件。”

传感器常见的分类方法对不同领域、不同行业对传感器的分类有可能不同，因为成百上千种传感器进行分类本身就是一门科学。但对传感器进行分类将有助于从总体上认识和掌握传感器，而且对传感器的开发与应用都是很有意义的。由于传感器的种类繁多，一种被测量，可以用不同的传感器来测量，而且传感器应用的原理又各种各样，同一原理的传感器，又可以测量多种被测量。因此，对传感器的分类是仁者见仁，智者见智。

1.5.3　性能评价与选用原则

（1）传感器的性能及其评价方法

理论直线法通常取零点作为理论直线的零点，满量程输出作为终点，这两点的连线即为理论直线。所以理论直线与实际测试点无关。端点直线法是将传感器标定数据的零点输出平均值和满量程输出平均值连成的直线作为拟合直线，这是一条特殊形式的理论直线。

最佳直线法是指使实际输出特性相对于所选拟合直线的最大正偏差等于最大负偏差的一条直线作为拟合直线。最小二乘法直线法是按最小二乘原理求取拟合直线，该直线能保证传感器校准数据的残差平方和最小。灵敏度 S 是指传感器在稳态下输出量增量与被测输入量增量之比，即

$$S=\frac{\Delta y}{\Delta x}=\frac{\mathrm{d}y}{\mathrm{d}x} \tag{1-1}$$

显然，线性传感器的灵敏度是拟合直线的斜率；非线性传感器的灵敏度，通常也是用拟合直线的斜率表示的，非线性特别明显的传感器灵敏度可以用 $\mathrm{d}y/\mathrm{d}z$ 表示，或用某一小（输入量）区间内拟合直线的斜率表示。

迟滞（滞后）特性是反映传感器正（输入量增大）反（输入量减小）行程过程中，输出—输入曲线的不重合程度，也就是说，对应同一大小的输入信号，传感器正反行程的输出信号的大小却不相等，这就是迟滞现象。产生这种现象的主要原因是传感器机械部分存在不可避免的缺陷，如轴承摩擦、间隙、紧固件松动、材料的内摩擦、积尘等。实际评价用正反行程输出的最大偏差 $(\Delta R)_{\max}$ 与满量程输出 Y_{FS} 的百分比来表示，即

$$\delta_{\mathrm{R}}=\pm\frac{(\Delta R)_{\max}}{Y_{\mathrm{FS}}}\times 100\% \tag{1-2}$$

重复性是衡量传感器在同一工作条件下，输入量按同一方向作全量程连续工作多次变动时，所得特性曲线间一致程度的指标。各条特性曲线越靠近，重复性就越好。重复性的好坏与许多随机因素有关，具有随机误差，要按统计规律来确定，用标定曲线间最大偏差 $(\Delta H)_{\max}$ 与满量程输出的百分比表示，即

$$\delta_{\mathrm{H}}=\pm\frac{(\Delta H)_{\max}}{Y_{\mathrm{FS}}}\times 100\% \tag{1-3}$$

分辨力是指传感器在规定测量范围内所能检测出被测输入量的最小变化量。有时对该值用满量程输入值的百分数表示，称为分辨率。

阈值是指能使传感器的输出端产生可测变化量的最小被测输入量值，即零点附近的分辨能力。有的传感器在零位附近有严重的非线性，形成所谓“死区”，则将“死区”的大小作为阈值；更多情况下，阈值主要取决于传感器噪声的大小，因而有的传感器只给出噪声电平。

稳定性又称长期稳定性，即传感器在相当长时间内仍保持其原性能的能力。用室温条件下传感器的输出与起始标定时的输出之间的差异来表示，有时也用标定的有效值来表示。

漂移是指在一定时间间隔内，传感器的输出存在着与被测输入量无关的、不需要的变化。漂移常包括零点漂移和灵敏度漂移。零点漂移或灵敏度漂移又分为时间漂移和温度漂移，即时漂和温漂。温漂是指由周围温度变化所引起的零点或灵敏度的变化。

相间干扰只存在于（两相或三相等）传感器中，一般地说若给其中一相加载，其他各相的输出应为零，但实际上其他相的输出端仍有信号输出，二者比值的百分数就是相间干扰。

静态误差是评价传感器静态特性的综合指标，指传感器在满量程内，任意一点输出值相对其理论值的可能偏离（逼近）程度。

（2）传感器的动态特性及其评价

动态特性是指传感器对随时间变化的输入量的响应特性。传感器的动态响应特性可以分为稳态响应特性和瞬态响应特性。

稳态响应特性是指传感器在振幅稳定不变的正弦形式非电量的作用下的响应特性。稳态响应的重要性，在于工程上所遇到的各种非电量变化曲线都可以展成傅里叶级数或进行傅里叶变换，即用一系列正弦曲线的叠加来表示原曲线。瞬态响应特性是指传感器在瞬变的非周期非电量作用下的响应特性。瞬变的波形多种多样，一般只选几种比较典型的规则波形，对传感器进行瞬态响应的分析。

截止频率和通频带是指当传感器的对数幅频特性曲线下降到零频率值以下 3dB 时，对应的频率为截止频率。传感器的幅值衰减−3dB 时，对应的频率范围称为传感器的通频带。

谐振频率和固有频率是指幅频特性曲线在某一频率处具有峰值，这个工作频率就是谐振频率，固有频率是指在无阻尼时，传感器的自由振荡频率。

传感器标定原则：为了达到标定的目标，标定的基准必须要有长期稳定而且精度高的基准。精度的传递对传感器进行标定，是根据试验数据确定传感器的各项性能指标，实际上也是确定传感器的测量精度。在标定传感器时，必须要有比被标定的传感器精度高的标准器，该标准的精度还必须要由比它更高精度的标准器进行定期的标定，而这个标准器则需要更高一级的标准器来标定。

互换性有些时候传感器的标定并不容易进行，作为经常使用的替换方法是对经过一定时间工作的传感器进行更换。

动态标定用于确定传感器的动态性能指标，对传感器进行动态标定有两个目的：一是了解传感器的动态响应特性，确定其性能指标，改进或更换传感器或对传感器进行动态补偿，采用能够对动态误差修正的技术对测试结果进行处理；二是当传感器的静态灵敏度与动态灵

敏度不同，或者传感器没有静态响应（如压电传感器）时，对传感器进行灵敏度标定。

传感器种类繁多，动态标定方法各异。下面介绍几种常用的标定方法。

1）冲击响应法具有所需设备少、操作简便、力值调整及波形控制方便的特点，因此被广泛采用。

2）频率响应法比较直观，精度比较高。但是需要性能优良的参考传感器，非电量正弦发生器的工作频率有限，实验时间长。

3）阶跃信号响应法。阶跃信号响应法的原理是，当传感器受到阶跃压力信号作用时，测得其响应，用基于机理分析的估计方法或实验建模方法求出传感器的频率特性、特征参数和性能指标。

（3）传感器的选用原则

传感器的选择方法：现代传感器在原理与结构上千差万别，如何根据具体的测量目的、测量对象以及测量环境合理地选用传感器，是在进行某个量测量时首先要解决的问题。当传感器确定之后，与之相配套的测量方法和测量设备也就可以确定了。

测试条件与目的：主要考虑被测量的选择、测量范围、过载的发生频度、测量要求精度、测量时间和输入信号的频带等。

传感器的性能：主要考虑精度、稳定性、响应速度、输出信号类型（模拟或数字）、静态特性、动态特性和环境特性，传感器的工作寿命或循环寿命、标定周期、信噪比等。

传感器应用中的注意事项：每一个传感器都有自己的性能和使用条件，因此对于特定传感器的适应性很大程度取决于传感器的使用方法。传感器的种类繁多，应用场合也各种各样，不可能将各种传感器的使用方法及注意事项一一列举。用户在使用传感器之前应特别阅读，消化说明书中的各项内容。其中主要的使用方法和注意事项如下。

1）正确地选择安装点和正确安装传感器都是非常重要的环节。若安装环节失误，轻者影响测量精度，重者会影响传感器的使用寿命，甚至损坏传感器。安装固定传感器的方式要简单可靠。传感器和测量仪表必须可靠连接，系统应有良好的接地，远离强电场、强磁场，传感器和仪表应远离强腐蚀性物体和易燃易爆物品。

2）传感器通过插头与供电电源和二次仪表连接时，应注意引线号不能接错、颠倒；连接传感器与测量仪表之间的连接电缆必须符合传感器及使用条件的要求。仪器输入端与输出端必须保持干燥和清洁，传感器不用时，应保持传感器插头和插座的清洁。

3）精度较高的传感器都需要定期校准，一般来说，需要 3～6 周校准一次。各种传感器都有一定的过载能力，但使用时应尽量不要超量程。在插拔仪表与外部设备连接线前，必须先切断仪表及相应设备电源。

4）传感器不使用时，应存放在温度为 10～35℃，相对湿度不大于 85%，无酸、无碱和无腐蚀性气体的房间内。

1.6 智能传感器与嵌入式系统

1.6.1 智能传感器

智能传感器（Intelligent sensor）是具有信息处理功能的传感器。智能传感器带有微处理机，具有采集、处理、交换信息的能力，是传感器集成化与微处理机相结合的产物。智能式传感器自 20 世纪 70 年代初出现以来，随着微处理器技术的迅猛发展及测控系统自动化、智能化的发展，要求传感器准确度高、可靠性高、稳定性好，而且具备一定的数据处理能力，并能够自检、自校、自补偿。传统的传感器已不能满足这样的要求。为制造高性能传感器，光靠改进材料工艺也很困难，需要利用计算机技术与传感器技术相结合来弥补不足。计算机技术使传感器技术发生了巨大变革，微处理器（或微计算机）和传感器相结合，产生了功能强大的智能式传感器。所谓智能式传感器，就是一种带有微处理机的，兼有信息检测、信号处理、信息记忆、逻辑思维与判断功能的传感器。一般智能机器人的感觉系统由多个传感器集合而成，采集的信息需要计算机进行处理，而使用智能传感器就可将信息分散处理，从而降低成本。与一般传感器相比，智能传感器具有以下三个优点：通过软件技术可实现高精度的信息采集，而且成本低；具有一定的编程自动化能力；功能多样化。

（1）智能传感器的典型结构

智能传感器主要由传感器、微处理器及其相关电路组成。传感器将被测的物理量转换成相应的电信号，送到信号调理电路中，进行滤波、放大、模—数转换后，送到微计算机中。计算机是智能传感器的核心，它不但可以对传感器测量数据进行计算、存储、数据处理，还可以通过反馈回路对传感器进行调节。由于计算机充分发挥各种软件的功能，可以完成硬件难以完成的任务，从而大大降低了传感器制造的难度，提高了传感器的性能以及降低成本。

如果从结构上划分，智能传感器可以分为集成式、混合式和模块式。集成智能传感器是将一个或多个敏感器件与微处理器、信号处理电路集成在同一硅片上，集成程度高，体积小，但目前的技术水平还很难实现；将传感器和微处理器、信号处理电路做在不同芯片上，则构成混合式智能传感器，目前这类结构较多；初级的智能传感器也可以由许多互相独立的模块组成，如将微计算机、信号调理电路模块、数据电路模块、显示电路模块和传感器装配在同一壳结构内组成模块式智能传感器。

（2）基于 SOC/IP 的智能传感器

智能传感器的特点是在功能上通过模拟人的感官和大脑的协调动作，结合长期以来测

试技术的研究和实际经验而提出来的。是一个相对独立的智能单元，它的出现对原来硬件性能的苛刻要求有所减轻，而靠软件帮助可以使传感器的性能大幅度提高。它是一门正在蓬勃发展的现代传感器技术，是涉及微机械和微电子技术、计算机技术、网络与通信技术、信号处理技术、电路与系统、传感技术、神经网络技术、信息融合技术、小波变换理论、遗传理论、模糊理论等多种学科的综合技术。

智能传感器中的智能功能主要涉及数字化的输出、信息存储与记忆、逻辑判断、决策、自检、自校、自补偿（基于微处理器）等技术。基于微处理器的智能传感器，从简单的数字化与信息处理已发展到了目前具有网络通信功能、神经网络、模糊理论、遗传理论、小波变换理论、多传感器信息融合等新理论、新技术逐步完善的现代智能传感器。智能传感器在技术实现中，除了传感器的信号处理外，传感器的接口技术以及数据采集系统中的智能传感器接口与协议也很重要。如在数据采集中智能传感器的蓝牙协议栈与 SoC 结构设计。传感器的智能化指传感器与微处理机可分为两个独立部分，传感器的输出信号经处理和转化后由接口送入微处理机部分进行运算处理。这类智能传感器主要由传感器、微处理器及其相关电路组成。传感器将被测的物理量转换成相应的电信号，送到信号处理电路中，进行滤波、放大、模—数转换后，送到微处理机中。

由系统 IC 向 SoC（System on ChIP）转变已成为历史发展的必然趋势。以 MEMS 为代表的新一代智能传感器技术，在与 SoC 技术相结合，用硬件实现了以往软件实现的功能，可能成为下一代智能传感器的代表。这是因为智能传感器需要硬件支持，SoC 与 MCU 相比，具有可靠性高、价格低、速度快、体积小、功能复用、保密性好等一系列特点。因为多数传统的 SoC 设计是以超深亚微米 IC 设计技术为基础的，可完成多数专用集成电路实现，其生产线和工艺稳定，精度高，成本低。这样，不仅可制造出高性能微控制器 MCU，还可实现数字和模拟两种输出。尤其对用户的特定需求（如组网式测量，自定义通信协议），还可在原产品基础上进行二次开发。优点是周期极短，为用户节省时间，提高效率；已广泛应用于压力传感器、温度传感器、加速度传感器以及陀螺等产品的制造之中，并在航空、航天、石油、化工、矿山、机械、大坝、地质、水文等行业等到充分的验证。

（3）复合传感器功能

1）复合敏感功能。我们观察周围的自然现象，常见的信号有声、光、电、热、力、化学等。敏感元件测量一般通过两种方式：直接和间接测量。而智能传感器具有复合功能，能够同时测量多种物理量和化学量，给出能够较全面反映物质运动规律的信息。如美国加利弗尼亚大学研制的复合液体传感器，可同时测量介质的温度、流速、压力和密度。美国 EG&amp；GICSensors 公司研制的复合力学传感器，可同时测量物体某一点的三维振动加速度、速度、位移，等等。

2）自补偿和计算功能。多年来从事传感器研制的工程技术人员一直为传感器的温度漂

移和输出非线性作大量的补偿工作，但都没有从根本上解决问题。而智能传感器的自补偿和计算功能为传感器的温度漂移和非线性补偿开辟了新的道路。这样，放宽传感器加工精度要求，只要能保证传感器的重复性好，利用微处理器对测试的信号通过软件计算，采用多次拟合和差值计算方法对漂移和非线性进行补偿，从而能获得较精确的测量结果。

3）自检、自校、自诊断功能。普通传感器需要定期检验和标定，以保证它在正常使用时具有足够的准确度，这些工作一般要求将传感器从使用现场拆卸送到实验室或检验部门进行。对于在线测量传感器出现异常则不能及时诊断。采用智能传感器情况则大有改观，首先自诊断功能在电源接通时进行自检，诊断测试以确定组件有无故障。其次根据使用时间可以在线进行校正，微处理器利用存在 EPROM 内的计量特性数据进行对比校对。

4）信息存储和传输。随着全智能集散控制系统（Smart Distributed System）的飞速发展，对智能单元要求具备通信功能，用通信网络以数字形式进行双向通信，这也是智能传感器关键标志之一。智能传感器通过测试数据传输或接收指令来实现各项功能。如增益的设置、补偿参数的设置、内检参数设置、测试数据输出等。

5）智能传感器的集成化。由于大规模集成电路的发展使得传感器与相应的电路都集成到同一芯片上，而这种具有某些智能功能的传感器叫做集成智能传感器。集成智能传感器的功能有三个方面的优点：较高信噪比；传感器的弱信号先经集成电路信号放大后再远距离传送，就可大大改进信噪比。改善性能；由于传感器与电路集成于同一芯片上，对于传感器的零漂、温漂和零位可以通过自校单元定期自动校准，又可以采用适当的反馈方式改善传感器的频响。信号规一化；传感器的模拟信号通过程控放大器进行规一化，又通过模数转换成数字信号，微处理器按数字传输的几种形式进行数字规一化，如串行、并行、频率、相位和脉冲等。

1.6.2 嵌入式系统

物联网的感知层使用大量的嵌入式感知设备，嵌入式技术是使物联网具有感知能力的基础。掌握嵌入式技术对于理解物联网的基本工作原理是非常重要的。嵌入式系统也称嵌入式计算机系统，它是针对特定的应用，剪裁计算机的软件和硬件，以满足应用系统对功能、可靠性、成本、体积、功耗要求的专用计算机系统。

嵌入式系统是将计算与控制的概念联系在一起，并嵌入到物理系统之中，实现智能化的目的。无线传感器网络是在嵌入式技术基础上实现环境智能化的重要技术领域，嵌入式系统通过采集和处理来自不同感知源的信息，实现对物理过程的控制，以及与用户的交互，嵌入式系统技术是实现智能化的基础性技术。

微型机应用和微处理器技术的发展为嵌入式系统奠定了基础，微型机应用技术的发展、微处理器芯片可定制、软件技术的发展都为嵌入式系统的诞生创造了条件，奠定了基础。

其技术特点是：

1）嵌入式系统在智能控制方面的应用。计算机系统分为通用计算机与嵌入式计算机两大系统。在物联网中面对的是大数据量、复杂计算的需求，要选择通用计算机系统，而面对环境中需要联入网中的大量设备，如 PDA、电视机顶盒、手机、数字电视、数字相机、汽车控制器、工业控制器、机器人、医疗设备中的智能控制，对作为其内部组成部分的计算机的功能、体积、耗电有特殊的要求，这种特殊的设计要求是推动定制的小型嵌入式计算机系统发展的动力。

2）嵌入式系统与微处理器及软件。由于嵌入式系统要适应 PDA、手机、汽车控制器、工业控制器、物联网端系统与医疗设备中不同的智能控制功能、性能、可靠性与体积等方面的要求，而传统的通用计算机的体系结构、操作系统、编程语言都不能够适应嵌入式系统的要求，因此研究人员必须为嵌入式系统研究特殊要求的微处理器芯片、嵌入式操作系统与嵌入式软件编程语言。

3）嵌入式系统人员的要求。因对象的特征不同，单纯的通用计算机的设计与编程能力不能满足嵌入式任务的要求，开发团队必须由计算机、机器人、电子学等多方面的技术人员组成。在实际工作中，为满足物联网的具体要求，从事嵌入式系统开发的技术人员要由两类人员组成：一类是电子工程、通信工程专业的技术人员，主要是完成硬件设计，开发与底层硬件关系密切的软件；另一类是从事计算机与软件专业的技术人员，主要从事嵌入式操作系统和应用软件的开发。这样才能同时具备硬件设计能力、底层硬件驱动程序、嵌入式操作系统与应用程序开发能力的复合型要求。

1.7　微传感器及 MEMS 技术

微电子机械系统或微机电一体化系统（MEMS），统称为微机电系统。MEMS 主要包括微型机构、微型传感器、微型执行器和相应的处理电路等部分，它是在融合多种微细加工技术，并应用现代信息技术的最新成果的基础上发展起来的高科技前沿学科。完整的 MEMS 是由微传感器、微执行器、信号处理和控制电路、通信接口和电源等部件组成的一体化的微型器件系统。其目标是把信息的获取、处理和执行集成在一起，组成具有多功能的微型系统，集成于大尺寸系统中，从而大幅度地提高系统的自动化、智能化和可靠性水平。

MEMS 是外形轮廓尺寸在毫米量级以下，构成它的机械零件和半导体元器件尺寸在微米/纳米量级，可对声、光、热、磁、运动等自然信息进行感知、识别、控制和处理的微型机电装置。它将微电机、微电路、微传感器、微执行器等微型装置和器件集成在硅片上。

这种微型机电系统不仅能够搜集、处理与发送信息或指令，还能够按照所获取的信息自主地或根据外部的指令采取行动。

（1）MEMS 的特点

1）微型化。MEMS 器件体积小、质量轻、耗能低、惯性小、谐振频率高、响应时间短。

以硅为主要材料，机械和电气性能优良。硅的强度、硬度和弹性模量与铁相当，密度类似铝，热传导率接近钼和钨。

2）批量生产。用硅微加工工艺在一片硅片上可同时制造成百上千个微型机电装置或完整的 MEMS。批量生产可大大降低生产成本。

3）集成化。可以把不同功能、不同敏感方向或制动方向的多个传感器或执行器集成于一体，或形成微传感器阵列、微执行器阵列，甚至把多种功能的器件集成在一起，形成复杂的微系统。微传感器、微执行器和微电子器件的集成可制造出可靠性、稳定性很高的 MEMS。

4）多学科交叉。MEMS 涉及电子、机械、材料、制造、信息与自动控制、物理、化学和生物等多种学科，并集约了当今科学技术发展的许多尖端成果。

（2）MEMS 的主要技术

MEMS 的核心是单片式或集成式芯片，这种芯片不仅具有感测功能（带有微传感器），而且还具有执行功能（带有微执行器）。也就是说，MEMS 是一个含有信息处理的三位一体装置的微系统。MEMS 所需的主要技术如图 1-9 所示。

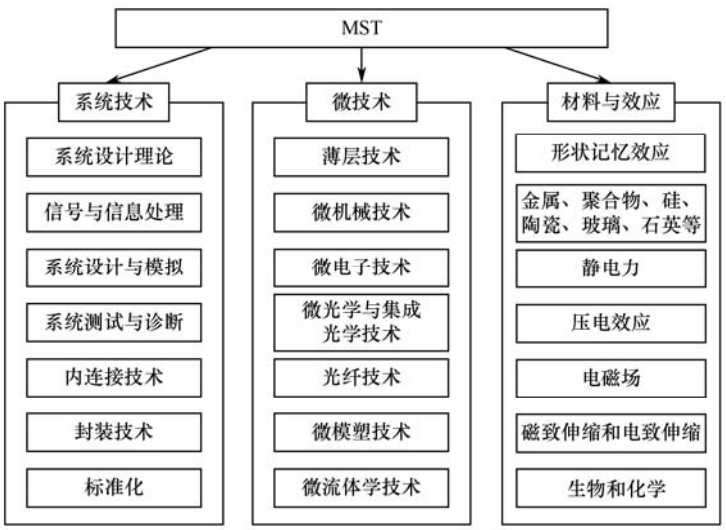


图 1-9　MEMS 所需的主要技术

构成这种微系统的技术称为微系统技术（MST）。早期的工作集中在硅技术上，并成功地制成了一些微机械装置，如压力传感器和喷墨打印机喷头。然而这些东西更准确的名称应该叫做装置，而不是 MEMS。完全意义上的 MEMS 之所以进展缓慢，是由于它的制作过程复杂。以微机械为研究对象的微机电系统涉及多种学科，主要有微机械学、微电子学、自动控制、物理、化学、生物等。随着检测对象和应用场合的不同，所用的基础理论、材料、设计及加工方法也不尽相同。

MEMS 的制作工艺技术主要基于两大技术，即 IC 技术和微机械加工技术，其中 IC 技术主要用于制作 MEMS 中的信号处理和控制系统，与传统的 IC 技术差别不大；而微机械加工技术则主要包括体微机械加工技术、表面微机械加工技术、LIGA 技术、准 LIGA 技术、芯片键合技术和微机械组装技术等。

MEMS 器件由早期的自然演变进入自身全面发展时期。人们开始提出一些新的设计理念，如微型飞机、微型机器人、微型汽车及微型潜艇等。这些复杂的 MEMS 器件，可以测定空间的位置与方向以及相对于其他物体的临近程度。它们还应具有与遥控操作人员的通信能力，因此需要一种无线通信链接装置（特别是要求它们进入人体内部时）。与 MEMS 器件发展相关联的一个主要问题是进一步解决合适的小型化电源。

（3）微传感器

微传感器是 MEMS 的一个重要组成部分。现在已经形成产品和正在研究中的有压力、力、力矩、加速度、速度、位置、流量、电量、磁场、温度、气体成分、湿度、pH 值、离子浓度和生物浓度、微陀螺、触觉传感器等。其中，力学量微传感器是微传感器最重要的种类，这是因为被测的力学量种类繁多并成功地大量用在市场上，如汽车工业市场。

迄今为止，力学量微传感器主要类别大体上分为六类，这六类产品占据大部分力学量微传感器的现有市场。这样，力学量微传感器的主要被测量是加速度/减速度、位移、流速、力/扭矩、位置/角度和压力/应力。

1）压力微传感器。压力微传感器是硅微机械加工制成的传感器的首要类型，是 20 世纪 50 年代末至 60 年代初开发出来的。因此，压力微传感器可以代表最成熟的硅微机械加工的器件，是至今最广泛的商品化产品。

因为单晶硅不会产生蠕变或迟滞现象，所以它是制作膜片的理想材料。在带有电容敏感组件的单晶硅压力传感器的一般结构中，电容电桥可由两个基准电容器组成，输出电压与膜片的偏移有关，因而又与施加的压力有关。表 1-1 总结了电容式压力传感器和压阻式压力传感器的优缺点。

表 1-1　电容式压力传感器和压阻式压力传感器的优缺点

类　型	优　点	缺　点
电容式压力传感器	更加灵敏（多晶硅）；温度影响较小；更加坚实	机械加工的硅片较大；电子装置比较复杂；必须有集成电路
压阻式压力传感器	结构比体电容式小；转换电路简单；无须集成	温度依赖性较强；压电系数取决于掺杂浓度

2）加速度微传感器。加速度微传感器基于悬臂梁原理，即末端质量块（或移动结构）在惯性力作用下产生位移。多晶硅表面微机械加工技术制作的电容式传感器和单晶硅微机械加工技术制作的传感器是最普遍的，一般具有高 g 值和低 g 值等各种器件。目前加速度微传感器的生产数以百万计，而且带有复杂的阻尼和过载保护装置。加速度微传感器的主要市场是自动刹车系统、悬架系统（0～2g）和气囊系统（可达 50g）。

通过增加微谐振器的阻尼和刚度可进一步增加动态范围，因此加速度微传感器可用在军事上，如导弹控制。

3）微陀螺仪。采用微机械加工方法制作的耦合谐振式陀螺仪可以测量目标方位变化。这种器件是用微机械加工技术制作的，微型质量由 P 掺杂的单晶硅制成并由微型扭转梁支撑。陀螺的外框架在恒定振幅下由静电驱动，内框架的运动可被感测出。用多晶硅表面微机械加工方法已经制作出更加先进的陀螺仪，如一些耦合谐振器陀螺仪样品，还有用于精确测量旋转速率的环形陀螺仪。基本方法引人注目，但需要采用深腐蚀技术才能制作出这种富有生命力的器件。

4）流量微传感器。在汽车、航天以及化学工业等许多领域中，测量气体（或液体）的流速非常重要。例如，了解发动机燃料流量或供给家庭锅炉用的气体流量。实际上有许多传统的方法可直接测量流量（如旋转的叶片），也可通过差压间接地测量流量（节流孔板、文丘里管和皮氏流速测定管）。这里关注的是利用新型微力学量传感器所进行的流量测量。用微传感器检测气体和液体流量的最普通的工作原理，是以 1911 年托马斯首次认定的热流传感器的理论为基础的。即用热电偶温度传感器在两端点监测电阻丝加热器至流动液体的每单位时间传输的热量（P_{h}）。当达到稳定状态时，质量流速 Q_{m} 与温度差（T_2-T_1）成正比，由此得出

$$Q_{\mathrm{m}}=\frac{\mathrm{d}m}{\mathrm{d}t}=\frac{P_{\mathrm{h}}}{C_{\mathrm{m}}}(T_2-T_1) \tag{1-4}$$

式中，C_{m} 为假定管壁上没有热损耗的流体的质量定压热容。

还有一种略有不同的方法是用悬臂梁取代了微型电桥，加热器与基底之间用一层聚酰亚胺进行热隔离。这样热敏二极管就取代了热敏电阻器，传感器集成于 CMOS 电路。虽然仍能测量高达 30m/s 的流速，但功率损耗大约是原来的一半。

这种商品化的微型流速传感器带有自身温度补偿，但是这种传感器必须根据不同的气体（或混合气体）进行校准，因为气体的密度和热容不同。

5）其他类型的流量传感器。它们涉及的范围从相对简单的器件（如以简易的 MOS 为基础的风速表）到新近改进的带有 $\sigma-\delta$ 温度调制装置比较复杂的器件。然而随着微流体学领域在 MEMS 中所占的地位越来越重要，硅流量传感器极有可能在未来几年里应用不断扩大。

（4）微执行器

微执行器是将电信号转换为非电量的微型器件。微电机是一种典型的微执行器，可分为旋转式和直线式两类，其他的微执行器还有微开关、微谐振器、微阀、微泵等。把微执行器分布成阵列可以扩大其应用领域。微执行器的驱动方式主要有静电驱动、压电驱动、电磁驱动、形状记忆合金驱动、热双金属驱动、热气驱动等。

1.8 并行处理与云计算

在互联网中，成千上万台计算机和服务器连接到网络公司，搭成了能进行存储、计算的数据中心形成如云一样的信息处理能力，云计算的概念由此产生。云计算可以理解成互联网中数不清的计算机群，用户可以通过互联网接入到这个庞大的数据处理能力的云中，可以随时获取、实时使用、按需扩展计算和存储资源，按实际使用的资源付费。

云计算工作模式如图 1-10 所示。云计算是一种基于互联网的计算模式，它将计算、数据、应用等资源作为服务通过互联网提供给用户。在云计算环境中，用户不需要了解“云”中基础设施的细节，不必具备相应的专业知识，也无须直接进行控制，而只需要关注自己真正需要什么样的资源，以及如何通过网络来得到相应的服务。

云计算的优点是安全、方便，共享的资源可以按需扩展。云计算提供了可靠、安全的数据存储中心，用户可以不用再担心数据丢失、病毒入侵。这种使用方式对于用户端的设备要求很低。用户可以使用一台普通的个人计算机，也可以使用一部手机，就能够完成用户需要的访问与计算。

1）各种用户的云计算。由于用户可以根据自己的需要，按需使用云计算中的存储与计算资源，因此云计算模式更适用于中小企业，可以降低中小企业的产品设计、生产管理、电子商务的成本。苹果公司推出的平板计算机 iPad 的关键功能全都聚焦在互联网上，包括浏览网页、收发电子邮件、观赏影片照片、听音乐和玩游戏。当有人质疑 iPad 的存储容量太小时，苹果公司的回答是：“当一切都可以在云计算中完成时，硬件的存储空间早已不是重点。”

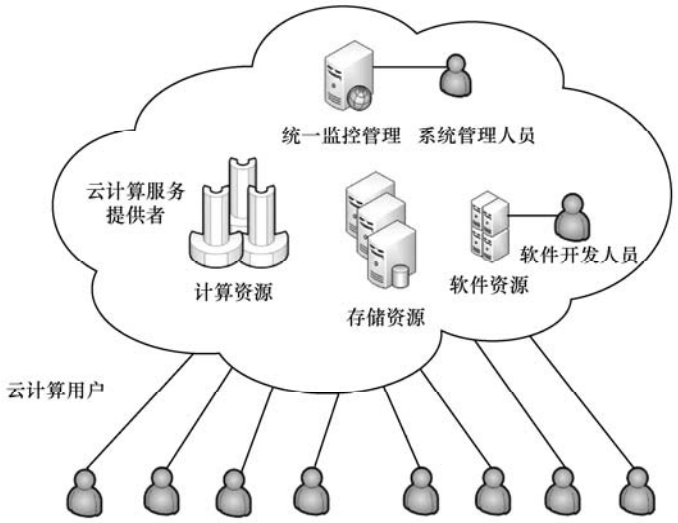


图 1-10　云计算工作模式示意图

2）云计算的软件服务。软件即服务（SaaS）是基于互联网的软件应用模式，是通过浏览器把程序传给成千上万的用户。从用户的角度将省去在服务器和软件购买授权方面的开支。从供应商的角度只需要维持一个程序就可以，从而降低了运营成本。云计算可以将开发环境作为一种服务向用户提供，使得用户能够开发出更多的互联网应用程序。

3）高性能计算、普适计算与云计算将成为物联网重要的计算环境。网格计算是随着互联网应用的发展而出现的一种专门针对复杂科学计算的新型计算模式。这种计算模式利用互联网将分散在不同地理位置的计算机组织成一台“虚拟的超级计算机”，其中每一个参与计算的计算机就是一个“结点”，而成千上万个结点就形成了一个“网格”。这种“虚拟的超级计算机”的特点是计算能力强，能够充分地利用互联网上空闲的计算资源。网格计算是超级计算机与计算机集群的延伸，它的应用主要是针对大型、复杂的科学计算问题。它们将计算变为一种公共设施，以服务租用的模式向用户提供服务，这些理念摆脱了传统自建信息系统的习惯模式。未来的网络应用，从手机、GPS 等移动装置，到搜索引擎、网络邮箱等基本的网络服务，以及大数据量的分析、大型物流的跟踪与规划、大型工程设计都可以通过云计算环境实现。

第 2 章　物联网中物体的标识、定位与时间同步

2.1　条码技术

2.1.1　一维条码技术

条码技术是在计算机技术与信息技术基础上发展起来的一门集编码、识别、采集和处理于一身的信息传感技术。条码技术主要研究条码标识信息 ean 码，并将条形码表示的信息转换成计算机可识读的语言，以实现自动输入、自动识读、自动统计。在先进的工业化国家中，条码技术作为一种信息处理技术已成为社会化产物，不仅应用于生产过程，而且也应用于管理过程。

一维条码是人们日常见到的印制在商品包装上直线装的条码，是国际统一的传统一维条码。这种条码在体系和标准上考虑得较充分，自 20 世纪 70 年代初期问世以来，很快在国际上得到普及并广泛地应用到工业、商业、国防、交通运输、金融、医疗卫生、邮电及办公室自动化等各个领域。

一维条码所代表的信息是由一组条、空按一定的规则排列来代表相应的字符所组成的。条码信息靠条和空的不同宽度和位置来传递，信息量的大小是由条码的宽度和印制的精度来决定的，条码越宽，包容的条和空越多，信息量越大；条码印制的精度越高，单位长度内可以容纳的条和空越多，传递的信息量也就越大。这种条码技术在一个方向上通过“条”与“空”的排列组合来存储信息，所以叫它为“一维条码”。这种用条、空组成的数据编码可以供机器识读，而且很容易译成二进制数和十进制数。

ean 码有两种类型：一种是标准版，另一种是缩短版。标准版表示 13 位数字，又称为 ean-13 码，缩短版表示 8 位数字，又称为 ean-8。两种条码的最后一位为校验位，由前面的

12 位或 7 位数字计算得出。两种版本的编码方式可参考国标 GB—12094—1998。ean 码由前缀码、厂商识别码、商品项目代码和校验码组成。前缀码是国际 ean 组织标识各会员组织的代码，我国为 690、691 和 692；厂商代码是 ean 编码组织在 ean 分配前缀码的基础上分配给厂商的代码；商品项目代码由厂商自行编码；校验码是为了校验代码的正确性。在编制商品项目代码时，厂商必须遵守商品编码的基本原则：对同一商品项目的商品必须编制相同的商品项目代码；对不同的商品项目必须编制不同的商品项目代码，以保证商品项目与其标识代码一一对应，即一个商品项目只有一个代码，一个代码只标识一个商品项目。

完整的一维条码通常都是由两侧的空白区、起始符、数据字符、校验符（可选）、终止符和供人识别字符组成的。一个条码符号的完整结构所包含的内容见表 2-1。

表 2-1　条码符号结构

空白区	起始字符	数据字符	校验字符	终止字符	空白区

图 2-1 所示为条码符号。一维条码符号中的数据字符和校验符是代表编码信息的字符，扫描识读后需要传输处理，左右两侧的空白区、起始字符、终止字符等都是不代表编码信息的辅助符号，仅供条码扫描识读时使用，不需要参与信息代码传输。

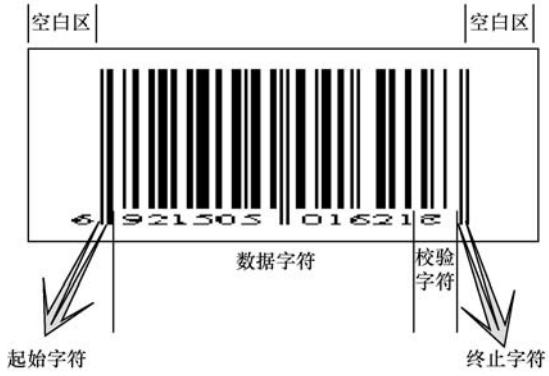


图 2-1　条码符号

商品条码的编码原则是采用国际通用的商品代码（international article numbexing__ean 代码）和北美地区通用的商品代码（universal product code_upc 代码）。两种代码在结构上有所不同，但均包括 5 位数字的商品项目代码。两种条码的编码原则是相同的，都是针对商品的项目代码而开展的编目。我国的一维条码主要采用的是 ean 代码，编码遵循的原则如下。

1）唯一性原则。是指商品项目与其标识代码一一对应，即一个商品项目只有一个代码，一个代码只标识同一商品项目。商品项目代码一旦确定，永不改变，即使该商品停止生产，停止供应了，在一段时间以内（一些国家规定为 3 年）也不得将该代码分配给

其他商品项目。在商品系统中商品及商品价格的差异是靠不同的代码识别的。唯一的商品项目代码与厂商代码和国别（地区）组配在一起就可以保证商品的代码标识在一个国家地区乃至全世界范围内都是唯一的。唯一性是商品编码最重要的一条原则，也是传统条码的局限所在。

2）无含义原则。是指代码数字本身及其位置不表示商品的任何特定信息。平常说的“流水号”就是一种无含义代码。在 ean 及 upc 系统中，商品编码仅仅是一种识别商品的手段，而不是商品分类的手段。无含义使商品编码具有简单、灵活、可靠、充分利用代码容量大、生命力强等特点，所以传统条码需要借助数据库的存在。

3）全数字型代码原则。是指在 ean 及 upc 系统中，商品编码全部采用阿拉伯字母。

条形码所反映的信息含义，是通用商品消费单元的编码信息。消费单元是指通过超级市场、百货商店、专业商店等零售渠道直接销售给最终用户的商品包装单元。定量消费单元是指以商品件数计价销售的消费单元，变量消费单元是指按基本计量单位计价，以随机数量销售的消费单元。消费单元的 ean 代码分为标准型和缩短型两种结构，这里具体说明标准型的编码规则。标准型 ean 代码由 13 位数字组成，称为 ean-13 代码，根据 ean 规范，这 13 位数字分别赋予了不同的含义。

条形码所反映的信息内容，前 3 位是国家代码，中间 4 位是生产商代码，后 5 位是产品代码，最后一位是自动生成的校验码。如中华人民共和国可用的国家代码有 690、691 和 692。其结构见表 2-2。

表 2-2　ean-13 代码结构

前缀码	厂商代码	商品项目代码	校验码
$p_1p_2p_3$	$m_1m_2m_3m_4$	$i_1i_2i_3i_4i_5$	c

例如，6901234567892，690 表示国家代码，1234 表示生产商代码，56789 表示产品代码，2 是校验码。

条码中的信息传感及信息的识读，主要传感装置是条码阅读机。装置的传感原理是利用光电传感器，采用逐行扫描的方式读取条码信息。再由光电式阅读传感器将信息传给相联系的处理器 CPU 来识别条码中所包含的信息。由于此种方式对遭污损的条码识读能力差，若要达到理想的识读效果，则对条码的印制质量要求高。同时，一维条形码只是在一个方向（一般是水平方向）表达信息，而在垂直方向则不表达任何信息，其一定的高度通常是为了便于阅读器的对准。尽管一维条形码的应用可以提高信息录入的速度，减少差错率，但是一维条形码也存在一些不足之处，例如：数据容量较小，只有 30 个字符左右；只能包含字母和数字；条形码尺寸相对较大（空间利用率较低）；条形码遭到损坏后便不能识读。为此经过进一步研究，开发出了二维条码技术。

2.1.2 二维条码技术

1. 二维条码及其特点

一维条码的信息容量小，条码仅能容纳几位或者几十位阿拉伯数字或字母，商品的详细描述只能依赖数据库提供，离开了预先建立的数据库，一维条码的使用就受到了局限。面对上述原因，人们迫切希望发明一种新的码制，除具备一维条码的优点外，同时还有信息容量大、可靠性高、保密防伪性强等优点。为了满足人们的这种需求，人们又推出了二维条码技术。

二维条码（2-dimensional barcode）是在水平和垂直方向的二维空间存储信息。二维条码具有信息容量大、可靠性强、保密性高、识别率高、编码范围广等特点。同一维条码相比，二维条码也有一些缺点，如要有专门的生成程序；识读设备价格比较昂贵；对于在线扫描，即先有码后赋值的模式，不能发挥其特点。

（1）二维条形码的分类

二维条形码与一维条形码一样，也有许多不同的编码方法，或称为码制。就这些码制的编码原理而言，通常可分为以下两种类型。

线性堆叠式二维码是在一维条形码编码原理的基础上，将多个一维码在纵向堆叠而产生的。典型的码制如 Code 16K、Code 49、PDF417（见图 2-2）等。

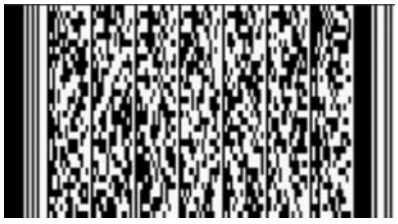


图 2-2　PDF417 二维条码

矩阵式二维码是在一个矩形空间通过黑、白像素在矩阵中的不同分布进行编码。典型的码制如 Aztec、Maxi Code、QR Code、Data Matrix 等。邮政编码通过不同长度的条进行编码，如 Postnet、BPO 4-State。

在许多种类的二维条形码中，常用的码制有：Data Matrix，Maxi Code，Aztec，QR Code，Vericode，PDF417，Ultracode，Code 49，Code 16K 等。Data Matrix 主要用于电子行业小零件的标识，如 Intel 的奔腾处理器的背面就印制了这种码。Maxi Code 是由美国联合包裹服务（UPS）公司研制的，用于包裹的分拣和跟踪。Aztec 是由美国韦林（Welch Allyn）公司推出的，最多可容纳 3832 个数字或 3067 个字母字符或 1914 个字节的数据。PDF417 码，PDF 是取英文 Portable Data File 三个单词的首字母的缩写，意为“便携数据文件”。因为组

成条形码的每一符号字符都是由 4 个条和 4 个空构成的，如果将组成条形码的最窄条或空称为一个模块，则上述的 4 个条和 4 个空的总模块数一定为 17，所以称为 417 码或 PDF417 码，它是由留美华人王寅敬（音）博士发明的。这种二维码有以下特点。

1）信息容量大。PDF417 码除可以表示字母、数字、ASCII 字符外，还能表达二进制数。为了使得编码更加紧凑，提高信息密度，PDF417 在编码时有三种格式：扩展的字母数字压缩格式，可容纳 1850 个字符；二进制/ASCII 格式，可容纳 1108 个字节；数字压缩格式，可容纳 2710 个数字。

2）错误纠正能力。一维条形码通常具有校验功能以防止错读，一旦条形码发生污损将被拒读。而二维条形码不仅能防止错误，而且能纠正错误，即使条形码部分损坏，也能将正确的信息还原出来。

3）印制要求不高。普通打印设备均可打印，传真件也能阅读。

4）可用多种阅读设备阅读。PDF417 码可用带光栅的激光阅读器、线性及面扫描的图像式阅读器阅读。

5）尺寸可调以适应不同的打印空间。

6）码制公开已形成国际标准，我国也已制定了 417 码的国标。

（2）二维条形码的特点

1）信息容量大。在一个二维条码中可以存储 1000 个字节以上，一个载体上可以有几个二维条码。

2）信息密度高。同样大小的二维条码是一维条码信息密度的 100 倍以上。

3）识别率极高。由于二维码有极强的错误修正技术，即便污损 50%的面积也能正确读出全部信息。

4）保密性、防伪能力强。由于二维码的编码技术十分巧妙，因此能非常有效地防止伪造；编码范围广，可以将照片、指纹、掌纹、手写签名等可以数字化的信息进行编码：制作容易，使用成本低。可以打印在普通的纸张、PVC 或其他材料上，与一维条码的制造成本相当。

（3）二维条码阅读器

二维条码的阅读设备依阅读原理的不同可分为：

1）线性 CCD 和线性图像式阅读器（Linear Imager）。可阅读一维条码和线性堆叠式二维码（如 PDF417），在阅读二维码时需要沿条码的垂直方向扫过整个条码，我们称为“扫动式阅读”。这类产品价格比较便宜，有很好的性价比。

2）带光栅的激光阅读器。可阅读一维条码和线性堆叠式二维码。阅读二维码时将光线对准条码，由光栅元件完成垂直扫描，不需要手工扫动。

3）图像式阅读器（Image Reader）。采用摄像方式将条码图像摄取后进行分析和解码，

可阅读一维条码和所有类型的二维条码，是一种高端设备。

美国 Hand Held Products 公司是世界上主要的条码阅读设备制造商之一，其 CCD 技术、图像式阅读器（Image Reader）技术以及译码技术处于世界领先地位，最近该公司又提出了线性图像（Linear Imaging）技术的新概念。以先进的技术为基础，HHP 公司的二维条码阅读设备一直引领着世界的潮流，其主要产品包括 IT3800 和 IT4600 等。

2. 二维条形码的应用

（1）运输行业的应用

典型的运输业务过程通常经历：供应商→货运代理→货运公司→客户等几个过程，在每个过程中都牵涉发货单据的处理。发货单据含有大量的信息，包括：发货人信息、收货人信息、货物清单、运输方式等。单据处理的前提是数据的录入，人工键盘录入的方式存在着效率低、差错率高的问题，已不能适应现代运输业的要求。

二维条形码在这方面提供了一个很好的解决方案，将单据的内容编成一个二维条形码，打印在发货单据上，在运输业务的各个环节使用二维条形码阅读器扫描条形码，信息便录入到计算机管理系统中，既快速又准确。

在美国，虽然 EDI 应用革新了业务流程的核心部分，但不巧的是它却忽略了流程中的关键角色——货运公司。许多 EDI 报文对于货运商来说总是迟到，以至于因不能及时确认准确的装运单信息而影响了货物运输和客户单据的生成。美国货运协会（ATA）因此提出了纸上 EDI 系统。发送方将 EDI 信息编成一张 PDF417 条形码标签提交给货运商，通过扫描条形码，信息立即传入货运商的计算机系统。这一切都发生在恰当的时间和恰当的地点，使得整个运输过程的效率大大提高。

（2）身份识别卡的应用

美国国防部已经在军人身份卡上印制 PDF417 码。持卡人的姓名、军衔、照片和其他个人信息被编成一个 PDF417 码印在身份卡上。身份卡被用于重要场所的进出管理及医院就诊管理。

该项应用的优点在于数据采集的实时性，低实施成本，卡片损坏（如枪击）也能阅读，以及防伪性。我国香港特别行政区的居民身份证也采用了 PDF417 码。其他的应用，如营业执照、驾驶执照、护照、我国城市的流动人口暂住证、医疗保险卡等也都是很好的应用方向。

（3）文件和表格应用

日本 Seimei 保险公司的每个经纪人在会见客户时都带着便携式计算机。每张保单和协议都在计算机中制作并打印出来。当经纪人回到办公室后需要将保单数据手工输入到公司的主机中。为了提高数据录入的准确性和速度，经纪人在制作保单的同时将保单内容编成一个 PDF417 条形码，打印在单据上，这样就可以使用二维条形码阅读器扫描条形码将数

据录入主机。其他类似的应用还有：海关报关单、税务申报单、政府部门的各类申请表等。

（4）资产跟踪

美国钢管公司在各地拥有不同种类的管道需要维护。为了跟踪每根钢管，公司将钢管的编号、位置编号、制造厂商、长度、等级、尺寸、厚度以及其他信息编成一个 PDF417 条形码，制成标签后贴在钢管上。当钢管移走或安装时，操作员扫描条形码标签，数据库信息得到及时更新。工厂可以采用二维条形码跟踪生产设备；医院和诊所也可以采用二维条形码标签跟踪设备、计算机及手术器械。

（5）混合码及其应用

随着社会的发展，科技的进步，人民生活水平的提高以及市场竞争的加剧，人们对信息的要求不断提高。一维条码在它的一些传统应用领域，如商业、药品、后勤运输等，由于受到信息容量的限制（一般只能标识物品或业务的识别号），已越来越不能满足人们的要求，而二维条码技术的不断完善正在这些应用领域引发着变革。

美国 UCC 组织（统一编码委员会）推出了一种新的码制——混合码，它是一种一维码和二维码的组合码，其中一维码组成部分可以是：UCC/EAN-128；UPC/EAN；Reduced Space Symbology（RSS）。二维码组成部分可以是：CC-A（一种专用于混合码的 PDF417 微码的变体）；CC-B（标准 PDF417 微码）；CC-C（标准 PDF417）。

混合码的应用包括以下几个方面。

1）混合码在后勤和运输业务中的应用。采用 UCC/EAN-128 并以二维条码作为补充，提供采购订单号、装运单、路线信息、装运通知的电子备份、包装、包含事项和批号等信息。

2）混合码在药品流通中的应用。用二维条码记录补充信息，可以提供过期日期以利于药品周转，同时可以记录批号用于药品跟踪。

3）混合码在零售业中的应用。在食品，特别是新鲜及冷冻的易坏的东西上标上批号和过期日期可以使得货物的周转效率大大提高。在电子产品上也可以标上软件和硬件的版本修订信息。

2.2　RFID 技术

2.2.1　RFID 的原理及特性

射频识别技术的优点在于可以以无接触的方式实现远距离、多标签甚至在快速移动的状态下进行自动识别。计算机网络技术的发展，尤其是互联网技术的发展使得全球信息传递的即时性得到了基本保证。在此基础上，人们开始将这两项技术结合起来应用于物品标

识和供应链的自动追踪管理，由此诞生了 EPC。当 EPC 标签贴在物品上或内嵌在物品中的时候，即将该物品与 EPC 标签中的唯一编号（标准说法是“产品电子代码”或“EPC 代码”）建立起了一对一的对应关系。

射频识别技术（RFID）的基本原理是利用射频信号及其空间耦合和传输特性，实现对静止或移动物体的自动识别。射频识别的信息载体是射频标签，其形式有卡、纽扣、标签等多种类型。射频标签贴在产品或安装在产品或物品上，由射频识读器读取存储于标签中的数据。RFID 可以用来追踪和管理几乎所有物理对象。因此，越来越多的零售商和制造商都在关心和支持这项技术的发展与应用。

采用 RFID 最大的好处是可以对企业的供应链进行高效管理，以有效地降低成本。因此，对于供应链管理应用而言，射频技术是一项非常适合的技术，但由于标准不统一等原因，该技术在市场中并未得到大规模的应用。因此，为了获得期望的效果，用户迫切要求开放标准。

（1）RFID 技术的优点

RFID 技术是用射频信号通过空间耦合（交变磁场或电磁场）实现无接触信息传递并通过所传递的信息达到识别目的的技术（电子标签是 RFID 的通俗叫法）。与目前广泛使用的自动识别技术如摄像、条码、磁卡、IC 卡等相比，RFID 的优点如下：

1）非接触操作，长距离识别（几厘米至几十米），识别工作无须人工干预，应用便利。

2）无机械磨损，寿命长，并可工作于各种油渍、灰尘污染等恶劣的环境。

3）可识别高速运动物体，并可同时识别多个电子标签。

4）读写器具有不直接对最终用户开放的物理接口，保证其自身的安全性。

5）数据安全方面除电子标签的密码保护外，数据部分可用一些算法实现安全管理。

6）读写器与标签之间存在相互认证的过程，可实现安全通信和存储。

目前，RFID 技术在工业自动化、物体跟踪、交通运输控制管理、防伪和军事方面已经有着广泛的应用。

（2）RFID 系统的组成

1）电子标签：由耦合组件及芯片组成，且每个电子标签具有全球唯一的识别号（ID），无法修改、无法仿造，这样就提供了安全性。电子标签附着在物体上来标识目标对象。电子标签中一般保存有约定格式的电子数据，在实际应用中，电子标签附着在待识别物体的表面。

2）天线：在电子标签和读写器间传递射频信号，即电子标签的数据信息。

3）读写器：读取（或写入）电子标签信息的设备，可设计为手持式或固定式。

读写器可无接触地读取并识别电子标签中所保存的电子数据，从而达到自动识别物体的目的。通常读写器与计算机相连，所读取的电子标签信息被传送到计算机上，进行下一步处理。

（3）RFID 的工作特性

1）数据的读/写（Read Write）机能。只要通过 RFID 阅读器即可不需接触，直接读取

信息至数据库内，且可一次处理多个标签，并可以将物流处理的状态写入标签，供下一阶段物流处理使用。

2）容易小型化和多样化的形状。RFID 在读取上并不受尺寸大小与形状的限制，不需为了读取精确度而配合纸张的固定尺寸和印制品质。此外，RFID 电子标签更可往小型化与多样化形态发展，以应用于不同产品。

3）耐环境性可重复使用。纸张受到脏污就会看不到，但 RFID 对水、油和药品等物质却有强力的抗污性。RFID 在黑暗或脏污的环境之中，也可以读取数据；由于 RFID 为电子数据，可以反复被覆写，因此可以回收标签重复使用。如被动式 RFID，不需要电池就可以使用，没有维护保养的需要。

4）穿透性。RFID 若被纸张、木材和塑料等非金属或非透明的材质包裹，还可以进行穿透性通信。不过如果是铁质金属，就无法进行通信。

5）数据的记忆容量大。数据容量会随着记忆规格的发展而扩大，未来物品所需携带的资料量越来越大，对卷标所能扩充容量的需求也增加，对此 RFID 不会受到限制。

6）系统安全与数据安全。将产品数据从中央计算机中转存到工件上将为系统提供安全保障，大大地提高了系统的安全性；通过校验或循环冗余校验的方法来保证射频标签中存储的数据准确性。

射频标签与读写器之间的数据交换构成的是一个无线数据通信系统。射频标签与读写器之间交换的是数据，由于采用无接触方式通信，还存在一个空间无线信道。因此，射频标签与读写器之间的数据交换构成的是一个无线数据通信系统。在这样的数据通信系统模型下，射频标签是数据通信的一方，读写器是通信的另一方。要实现安全、可靠、有效的数据通信目的，数据通信的双方必须遵守相互约定的通信协议。没有这样一个通信双方公认的基础，数据通信的双方将互相听不懂对方在说什么，步调也无从协调一致，从而造成数据通信无法进行。

所涉及的主要问题包括：时序系统问题；通信握手问题；数据帧问题；数据编码问题；数据的完整性问题；多标签读写防冲突问题；干扰与抗干扰问题；识读率与误码率问题；数据的加密与安全性问题；读写器与应用系统之间的接口问题。

（4）RFID 信息的写入方式

射频标签读写装置的基本功能是无接触读取射频标签中的数据信息。从功能角度来说，单纯实现无接触读取射频标签信息的设备称为阅读器、读出装置、扫描器等。单纯实现向射频标签内存中写入信息的设备称为编程器、写入器等。综合具有无接触读取与写入射频标签内存信息的设备称为读写器、通信器等。射频标签信息的写入方式大致可以分为以下三种类型。

1）射频标签在出厂时，即已将完整的标签信息写入标签。这种情况下，在应用过程中，

射频标签一般具有只读功能。只读标签信息的写入，在更多的情况下是在射频标签芯片的生产过程中即标签信息写入芯片，使得每一个射频标签拥有一个唯一的标识 UID（如64Bits）。应用中，需再建立标签唯一 UID 与待识别物品的标识信息之间的对应关系（如车牌号）。只读标签信息的写入也有在应用之前，由专用的初始化设备将完整的标签信息写入。

2）射频标签信息的写入采用有线接触方式实现，一般称这种标签信息写入装置为编程器。这种接触式的射频标签信息写入方式通常具有多次改写的能力。例如，目前在用的铁路货车电子标签信息的写入即为这种方式。标签在完成信息注入后，通常需将写入口密闭起来，以满足应用中对其防潮、防水、防污等要求。

3）射频标签在出厂后，允许用户通过专用设备以无接触的方式向射频标签中写入数据信息。这种专用写入功能通常与射频标签读取功能结合在一起形成射频标签读写器。具有无线写入功能的射频标签通常也具有其唯一的不可改写的 UID。这种功能的射频标签趋向于一种通用射频标签，应用中可根据实际需要仅对其 UID 进行识读或仅对指定的射频标签内存单元（一次读/写的最小单位）进行读/写。

实际应用中还广泛存在着一次写入多次读出 WORM（Write Once Read Many）的射频标签。这种 WORM 概念即有接触式改写的射频标签存在，也有无接触式改写的射频标签存在。这类 WORM 标签一般大量用在一次性使用的场合，如航空行李标签、特殊身份证件标签等。

无论是怎样的情况，对射频标签的写操作均应在一定的授权控制之下进行。否则，将失去射频标签标识物品的意义。高频标签对人体有辐射。射频技术使用电磁波低端频谱，解读器发出的无线电波和汽车中的立体声一样安全无害。每个国家都有控制能量水平的机构，介于 AM 和 FM 之间的 13.56MHz 频率已经被使用多年，即使在很高的能量下也没有出现问题。美国和其他大多数国家的能量极限是 4W。模拟移动电话发出的频率是 915MHz，最新移动电话产生的频率为 2.45GHz。能量在 1W 以下没有被证明有危害健康的因素。

2.2.2 RFID 的组成

1. 电子标签

电子标签是射频识别系统的数据载体，电子标签由标签天线和标签专用芯片组成。依据电子标签供电方式的不同，电子标签可以分为有源电子标签（Active tag）、无源电子标签（Passive tag）和半无源电子标签（Semi-passive tag）。有源电子标签内装有电池，无源射频标签没有内装电池，半无源电子标签部分依靠电池工作。

电子标签依据频率的不同可分为低频电子标签、高频电子标签、超高频电子标签和微波电子标签。依据封装形式的不同可分为信用卡标签、线形标签、纸状标签、玻璃管标签、圆形标签及特殊用途的异形标签等。

从纯技术的角度来说，射频识别技术的核心在电子标签，阅读器是根据电子标签的设

计而设计的。不是任意形状都能满足阅读距离及工作频率的要求，必须根据系统的工作原理，即磁场耦合（变压器原理）还是电磁场耦合（雷达原理），设计合适的天线外形及尺寸。标签芯片即相当于一个具有无线收发功能再加存储功能的单片系统。虽然，在射频识别系统中电子标签的价格远比阅读器低，但通常情况下，在应用中电子标签的数量是很大的，尤其是物流应用中，电子标签可能是海量并且是一次性使用的，而阅读器的数量则相对要少得多。

实际应用中，电子标签除了具有数据存储量、数据传输速率、工作频率、多标签识读特征等电学参数之外，还根据其内部是否需要加装电池及电池供电的作用而将电子标签分为无源标签、半无源标签和有源标签三种类型。无源标签没有内装电池，在阅读器的阅读范围之外时，标签处于无源状态，在阅读器的阅读范围之内时标签从阅读器发出的射频能量中提取其工作所需的电能。半无源标签内装有电池，但电池仅对标签内要求供电维持数据的电路或标签芯片工作所需的电压作辅助支持，标签电路本身耗电很少。标签未进入工作状态前，一直处于休眠状态，相当于无源标签。标签进入阅读器的阅读范围时，受到阅读器发出的射频能量的激励，进入工作状态时，用于传输通信的射频能量与无源标签一样源自阅读器。有源标签的工作电源完全由内部电池供给，同时标签电池的能量供应也部分地转换为标签与阅读器通信所需的射频能量。

射频识别系统的另一主要性能指标是阅读距离，也称为作用距离，它表示在多远的距离上，阅读器能够可靠地与电子标签交换资讯，即阅读器能读取标签中的数据。实际系统中这一指标相差很大，取决于标签及阅读器系统的设计、成本的要求、应用的需求等，范围为 0～100m。典型的情况是，在低频 125kHz、13.56MHz 频点上一般均采用无源标签，作用距离在 10～30cm，个别有到 1.5m 的系统。在高频 UHF 频段，无源标签的作用距离可达到 3～10m。更高频段的系统一般均采用有源标签。

2. RFID 阅读器

（1）RFID 阅读器原理

通过天线与 RFID 电子标签进行无线通信，可以实现对标签识别码和内存数据的读出或写入操作。典型的阅读器包含有高频模块（发送器和接收器）、控制单元以及阅读器。

射频识别系统的基本模型如图 2-3 所示。其中，电子标签又称为射频标签、应答器、数据载体；阅读器又称为读出装置、扫描器、通信器、读写器（取决于电子标签是否可以无线改写数据）。电子标签与阅读器之间通过耦合元件实现射频信号的空间（无接触）耦合。在耦合通道内，根据时序关系，实现能量的传递、数据的交换。发生在阅读器和电子标签之间的射频信号的耦合类型有两种。

1）电感耦合。变压器模型，通过空间高频交变磁场实现耦合，依据的是电磁感应定律。

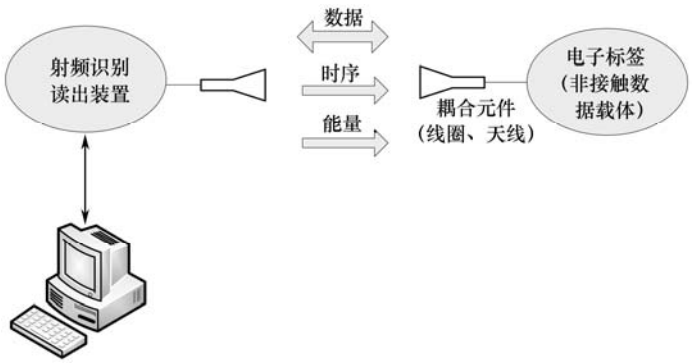


图 2-3　射频识别系统基本模型

2）电磁反向散射耦合。采用雷达原理模型，发射出去的电磁波，碰到目标后反射，同时携带回目标信息，依据的是电磁波的空间传播规律。

电感耦合方式一般适合中、低频工作的近距离射频识别系统。典型的工作频率有：125kHz、225kHz 和 13.56MHz。识别作用距离小于 1m，典型作用距离为 10～20m。电磁反向散射耦合方式一般适合高频、微波工作的远距离射频识别系统。典型的工作频率有：433MHz、915MHz、2.45GHz 和 5.8GHz。识别作用距离大于 1m，典型作用距离为 3～10m。

（2）RFID 读写器防冲撞机理

RFID 分类的第二个重要看点在于是否需要同时读取复数个标签。首先，为了实现这个功能在通信上所采取的技术是防碰撞（防冲撞），同时读取复数个标签是常被人们谈及的 RFID 比图形码远为优越的方面，但是如果没有防碰撞（防冲撞）的功能时，RFID 系统只能读写一个标签。在这种情况下，如果有两个以上的标签同时处于可读取的范围内就会导致读取的错误。

其次，我们来简单地说明防碰撞（防冲撞）功能的工作原理。即使是具有防碰撞（防冲撞）功能的 RFID 系统，实际上并非同时读取所有标签的内容。在同时查出有复数个标签存在的情况下，检索信号并防止冲突的功能开始动作。为了进行检索，首先要确定检索条件。例如，13.56MHz 频带的 RFID 系统里应用的 ALOHA 方式的防碰撞功能的工作步骤如下：

阅读器指定电子标签内存的特定位数（1～4 位）为次数批量。

电子标签根据次数批量，将响应的时机离散化。例如，在两位数的次数批量“00、01、10、11”时，读写器将以不同的时机对这 4 种可能性逐一进行响应。

若在各个时机里同时响应的电子标签只有一个的场合下才能得到这个电子标签的正常数据。信息读取之后阅读器对于这个电子标签发送在一定的时间内不再响应的睡眠指令（Sleep/Mute）使之再休眠，避免再次响应。

若在各个时机内同时由几个电子标签响应，则判别为“冲突”。在这种情况下，内存内的另外两位数所记录的次数批量，重复以上步骤。

所有的电子标签都完成响应之后，阅读器发送唤醒的指令（Wake Up），从而完成对所有电子标签的信息读取。

在这种搭载有防碰撞（防冲撞）功能的 RFID 系统中，为了只读一个标签，几经调整次数批量反复读取进行检索。所以，在一次性读取具有一定数量的标签的情况下，所有的标签都被读到其速度是不同的，一次性读取的标签数目越多，完成读取所需的时间要比单纯计算所需的时间越长。

实现防止抗碰撞（防冲撞）的功能是 RFID 在物流领域中取代图形码所必不可少的条件。例如，在超市中，商品是装在购物车里面进行计价的。为了实现这种计价方式，抗碰撞（防冲撞）功能必须完备。另外，在电子货币和个人认证方面利用 RFID 系统时，同时识别几个标签是发生差错的主要原因。

具有抗碰撞（防冲撞）功能的 RFID 系统的价格比不具有这种功能的系统的要昂贵。当个人用户在制作 RFID 系统的时候，如果没有必要进行复数个 ID 同时认识时就没有必要选择抗碰撞机能的读写器。

3. RFID 系统的天线

RFID 系统天线根据天线在系统中的不同功能和作用，RFID 中的天线可分为标签天线（tag antenna）和读写器天线（reader antenna）。标签天线不仅作为标签应答器的天线，将标签所存储的信息调制反射，同时还要捕获读写器发射的电磁波，为标签应答器提供能量。由于标签要能够粘贴到被识别的物体上，这就需要标签足够小，标签天线也就要求小尺寸，大多数情况下需要标签天线全向或半球覆盖的方向性，由于标签芯片的阻抗一般不是 50Ω，这就需要标签天线能够实现非 50Ω 与芯片阻抗的共扼匹配，以提供最大功率给芯片。一般情况下，标签需要大规模使用，这就要求标签天线成本低，加工简单。

读写器天线发射电磁能量以激活标签，实现数据传输向标签发出指令，同时也要接收来自标签的信息。一般地，由于被识别物体的空间指向可能无法固定，或标签的粘贴方式不确定，这就要求读写器天线为圆极化天线，可以实现物体空间指向发生变化时，不会出现极化完全失去匹配。同时，读写器天线还要求低剖面、小型化，有的要求多频段，甚至于有的读写器需要使用多天线技术，或智能波束扫描天线阵技术。

（1）天线的种类

RFID 天线主要有线圈型、微带贴片型、偶极子型三种基本形式。其中，小于 1m 的近距离应用系统 RFID 天线一般采用工艺简单、成本低的线圈型天线，它们主要工作在中低频段。而 1m 以上远距离的应用系统需要采用微带贴片型或偶极子型的 RFID 天线，它们工作在高频及微波频段。这几种类型天线的工作原理是不相同的。

1）线圈天线。

当 RFID 的线圈天线进入读写器产生的交变磁场中，RFID 天线与读写器天线之间的相互作用就类似于变压器，两者的线圈相当于变压器的初级线圈和次级线圈。由 RFID 的线圈天线形成的谐振回路包括 RFID 天线的线圈电感 L、寄生电容 C_p 和并联电容 C_2，其谐振频率为 $f=\dfrac{1}{2\pi\sqrt{L\cdot C}}$，式中 C 为 C_p 和 C_2 的并联等效电容。RFID 应用系统就是通过这一频率载波实现双向数据通信的。

某些应用要求 RFID 天线线圈外形很小，且需一定的工作距离，如用于动物识别的 RFID。线圈外形面积小的话，RFID 与读写器间的天线线圈互感量 M 就明显不能满足实际使用。通常在 RFID 的天线线圈内部插入具有高导磁率的铁氧体材料，以增大互感量，从而补偿线圈横截面减小的问题。

2）微带贴片天线。

微带贴片天线是由贴在带有金属板的介质基片上的辐射贴片导体所构成的，如图 2-4 所示。根据天线辐射特性的需要，可以设计贴片导体为各种形状。通常贴片天线的辐射导体与金属地板距离为几十分之一波长。假设辐射电场沿导体的横向与纵向两个方向没有变化，仅沿约为半波长的导体长度方向变化，则微带贴片天线的辐射基本上是由贴片导体开路边沿的边缘场引起的。由于辐射方向基本确定，因此一般适用于通信方向变化不大的 RFID 应用系统中。

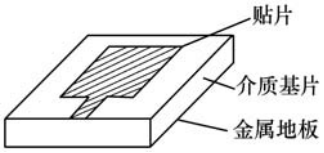


图 2-4　微带天线

3）偶极子天线。

在远距离耦合的 RFID 应用系统中，最常用的是偶极子天线，又称为对称振子天线。偶极子天线及其演化形式如图 2-5 所示。其中偶极子天线由两段同样粗细和等长的直导线排成一条直线构成，信号从中间的两个端点馈入，在偶极子的两臂上将产生一定的电流分布，这种电流分布就在天线周围空间激发起电磁场。

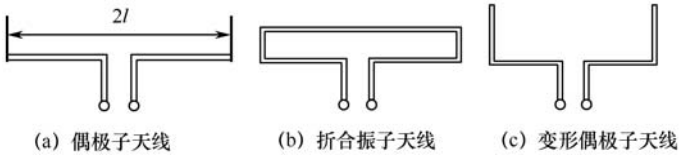


图 2-5　偶极子天线

利用麦克斯韦方程就可以求出其辐射场方程：

$$E_\theta = \int_{-1}^{1} \mathrm{d}E_\theta = \int_{-1}^{1} \frac{60\alpha I_z}{r} \sin\theta \cos(\alpha z \cos\theta)\mathrm{d}z$$

式中，I_z 为沿振子臂分布的电流，α为相位常数，r 为振子中点到观察点的距离，θ为振子轴到 r 的夹角，l 为单个振子臂的长度。同样也可以得到天线的输入阻抗、输入回波损耗、阻抗带宽和天线增益等特性。

当单个振子臂的长度半波振子 $l = \lambda/4$ 时，输入阻抗的电抗分量为零。天线输入阻抗可视为一个纯电阻，在忽略天线粗细的横向影响下，简单的偶极子天线设计可以取振子的长度 l 为 $\lambda/4$ 的整数倍。

（2）天线设计

在天线设计时主要考虑天线的类型和天线的阻抗，应用到物品上 RF 的性能，以及物品周围对 RF 性能影响等。下面我们分别做介绍。

1）阻抗的选择。

为了传输最大功率，天线后的芯片输入阻抗必须和天线的输出阻抗匹配。几十年来，设计天线与 50Ω 或 70Ω 的阻抗匹配，但是可能设计天线具有其他的特性阻抗。例如，一个缝隙天线可以设计具有几百欧姆的阻抗。一个折叠偶极子的阻抗可以是一个标准半波偶极子阻抗的 20 倍。印制贴片天线的引出点能够提供一个很宽范围的阻抗（通常是 40～100Ω）。选择天线的类型，以至于它的阻抗能够和标签芯片的输入阻抗匹配是十分关键的。另一个问题是其他的与天线接近的物体可以降低天线的返回损耗。对于全向天线，例如双偶极子天线，这个影响是显著的。其他的物体也有相似的影响。此外是物体的介电常数，而不是金属改变了谐振频率。可以设计天线使它与接近物体的情况相匹配，但是天线的设计对于不同的物体和不同的物体距离而不同。对于全向天线是不可行的，所以应设计方向性强的天线，它们不受这个问题的影响。

2）局部结构的影响。

在使用手持仪器时，大量的其他邻近物体使读卡机天线和标签天线的辐射模式严重失真。在仓库的使用环境下，一个物品盒子具有一个标签会有问题，几个标签贴在一个盒子上以确保所有时候都有一个标签是可以看见的。便携系统的使用有几个天线的问题。每个盒子具有两个天线足够适合门禁装置探测，这样局部结构的影响变得不再重要，因为门禁装置的读卡机天线被固定在仓库的出入处，并且直接指向贴标签的物体。

3）辐射模式。

在无反射的环境中测试天线的模式，包括各种需要贴标签的物体，在使用全向天线的时候性能会严重下降。圆柱金属引起的性能下降是最严重的。

4）距离。

RFID 天线的增益和是否使用有源的标签芯片将影响系统的使用距离。乐观的考虑，在电磁场的辐射强度符合 UK 的相关标准时，在 2.45GHz 的无源情况下，全波整流，驱动电压不大于 3V，优化的 RFID 天线阻抗环境（阻抗为 200～300Ω），使用距离大约是 1m。如果使用 WHO 限制则更适合全球范围的使用，但是作用距离下降了一半。这些限制了读卡机到标签的电磁场功率。作用距离随着频率升高而下降。如果使用有源芯片，则作用距离可以达到 5～10m。

全向天线应该避免在标签中使用，可以使用方向性天线，它具有更少的辐射模式和返回损耗的干扰。天线类型的选择必须使它的阻抗与自由空间和 ASIC 匹配。在一个仓库中使用天线好像是不可行的，除非使用有源标签，但是在任何情况下，仓库内的天线辐射模式将严重失真。一个门禁系统的使用将是好的选择，可以使用短作用距离的无源标签。当然，门禁系统价格比手持的仪器昂贵，但是手持仪器工作人员需要使用它到仓库搜寻物品，人员费用同样昂贵。在门禁系统中，每一个物品盒子，仅需要两个而不是 4 个或 6 个 RFID 标签。

5）耦合特性。

射频识别系统中射频标签与读写器之间的作用距离是射频识别系统应用中的一个重要问题，通常情况下这种作用距离定义为射频标签与读写器之间能够可靠交换数据的距离。射频识别系统的作用距离是一项综合指标，与射频标签及读写器的配合情况密切相关。由射频识别系统作用距离的远近，射频标签天线与读写器天线之间的耦合可分为三种类型。

① 密耦合。密耦合系统的典型作用距离范围为 0～1cm。实际应用中，通常需要将射频标签插入阅读器中或将其放置到读写器的天线的表面。密耦合系统利用的是射频标签与读写器天线无功近场区之间的电感耦合（闭合磁路）来构成无接触的空间信息传输射频通道工作的。密耦合系统的工作频率一般局限在 30MHz 以下的任意频率。由于密耦合方式的电磁泄漏很小，耦合获得的能量较大，因而可适合对要求安全性较高、作用距离无要求的应用系统，如电子门锁等。

② 遥耦合。遥耦合系统的典型作用距离可以达到 1m。遥耦合系统又可细分为近耦合系统（典型作用距离为 15cm）与疏耦合系统（典型作用距离为 1m）两类。遥耦合系统利用的是射频标签与读写器天线无功近场区之间的电感耦合（闭合磁路）来构成无接触的空间信息传输射频通道工作的。遥耦合系统的典型工作频率为 13.56MHz，也有一些其他频率，如 6.75MHz、27.125MHz 等。遥耦合系统目前仍然是低成本射频识别系统的主流。

③ 远距离耦合。远距离耦合的典型作用距离为 1～10m，个别的系统具有更远的作用距离。所有的远距离系统均是利用射频标签与读写器天线辐射远场区之间的电磁耦合（电磁波发射与反射）来构成无接触的空间信息传输射频通道工作的。远距离系统的典型工作频率为 915MHz、2.45GHz、5.8GHz。此外，还有其他一些频率，如 433MHz 等。远距离系

统的射频标签根据其中是否包含电池分为有无源射频标签（不含电池）和半无源射频标签（内含电池）。一般情况下，包含有电池的射频标签的作用距离较无电池的射频标签的作用距离要远一些。半无源射频标签中的电池并不是为射频标签和读写器之间的数据传输提供能量，而是只给射频标签芯片提供能量，为读写存储数据服务。

远距离耦合系统一般情况下均采用反射调制工作方式来实现射频标签到读写器方向的数据传输。远距离系统一般具有典型的方向性，射频标签与读写器成本目前还处于较高的水平。从技术角度来说，满足以下特点的远距离系统是理想的射频识别系统：射频标签无源；射频标签可无线读/写；射频标签与读写器支持多标签读/写；适合应用于高速移动物体的识别（物体移动速度大于 80km/h）；远距离（读写距离大于 5～10m）；低成本（可满足一次性使用要求）；现实的远距离系统一般均只能满足其中的几款要求。

2.2.3　RFID 工作频率与分类

射频标签的工作频率也就是射频识别系统的工作频率。毫无疑问，射频标签的工作频率是其最重要的特点之一。射频标签的工作频率不仅决定着射频识别系统工作原理（电感耦合还是电磁耦合）、识别距离，还决定着射频标签及读写器实现的难易程度和设备的成本。

工作在不同频段或频点上的射频标签具有不同的特点。射频识别应用占据的频段或频点在国际上有公认的划分，即位于 ISM 波段之中。典型的工作频率有 125kHz、133kHz、13.56MHz、27.12MHz、433MHz、902～928MHz、2.45GHz、5.8GHz 等。

从应用概念来说，射频标签的工作频率也就是射频识别系统的工作频率。

（1）低频段射频标签

低频段射频标签，简称低频标签，其工作频率范围为 30～300kHz。典型工作频率有 125kHz、133kHz。低频标签一般为无源标签，其工作能量通过电感耦合方式从阅读器耦合线圈的辐射近场中获得。低频标签与阅读器之间传送数据时，低频标签需位于阅读器天线辐射的近场区内。低频标签的阅读距离一般情况下小于 1m。

低频标签的典型应用有：动物识别、容器识别、工具识别、电子闭锁防盗（带有内置应答器的汽车钥匙）等。与低频标签相关的国际标准有：ISO11784/11785（用于动物识别）、ISO18000—2（125～135kHz）。低频标签有多种外观形式，应用于动物识别的低频标签外观有：项圈式、耳牌式、注射式、药丸式等。典型应用的动物有牛、信鸽等。

低频标签的主要优势体现在：标签芯片一般采用普通的 CMOS 工艺，具有省电、廉价的特点；工作频率不受无线电频率管制约束；可以穿透水、有机组织、木材等；非常适合近距离的、低速度的、数据量要求较少的识别应用（如动物识别）等。

低频标签的劣势主要体现在：标签存储数据量较少；只能适合低速、近距离识别应用；与高频标签相比，标签天线匝数更多，成本更高一些。

（2）中高频段射频标签

中高频段射频标签的工作频率一般为 3～30MHz。典型工作频率为 13.56MHz。该频段的射频标签，从射频识别应用角度来说，因其工作原理与低频标签完全相同，即采用电感耦合方式工作，所以宜将其归为低频标签类中。另外，根据无线电频率的一般划分，其工作频段又称为高频，所以也常将其称为高频标签。鉴于该频段的射频标签可能是实际应用中最大量的一种射频标签，因而我们只要将高、低理解成为一个相对的概念，即不会在此造成理解上的混乱。为了便于叙述，我们将其称为中频射频标签。

中频标签一般也采用无源标签，其工作能量同低频标签一样，也是通过电感（磁）耦合方式从阅读器耦合线圈的辐射近场中获得。标签与阅读器进行数据交换时，标签必须位于阅读器天线辐射的近场区内。中频标签的阅读距离一般情况下也小于 1m。

中频标签由于可方便地做成卡状，典型应用包括：电子车票、电子身份证、电子闭锁防盗（电子遥控门锁控制器）等。相关的国际标准有：ISO14443、ISO15693、ISO18000—3（13.56MHz）等。

中频标准的基本特点与低频标准相似，由于其工作频率的提高，可以选用较高的数据传输速率。射频标签天线设计相对简单，标签一般制成标准卡片形状。

（3）超高频与微波标签

超高频与微波频段的射频标签，简称微波射频标签，其典型工作频率为：433.92MHz、862（902）～928MHz、2.45GHz、5.8GHz。微波射频标签可分为有源标签与无源标签两类。工作时，射频标签位于阅读器天线辐射场的远区场内，标签与阅读器之间的耦合方式为电磁耦合方式。阅读器天线辐射场为无源标签提供射频能量，将有源标签唤醒。相应的射频识别系统阅读距离一般大于 1m，典型情况为 4～6m，最远可达 10m 以上。阅读器天线一般均为定向天线，只有在阅读器天线定向波束范围内的射频标签可被读/写。

由于阅读距离的增加，应用中有可能在阅读区域中同时出现多个射频标签的情况，从而提出了多标签同时读取的需求，进而这种需求发展成为一种潮流。目前，先进的射频识别系统均将多标签识读问题作为系统的一个重要特征。

以目前技术水平来说，无源微波射频标签比较成功，产品相对集中在 902～928MHz 工作频段上。2.45GHz 和 5.8GHz 射频识别系统多以半无源微波射频标签产品面世。半无源标签一般采用纽扣电池供电，具有较远的阅读距离。

微波射频标签的典型特点主要集中在是否无源、无线读/写距离、是否支持多标签读/写、是否适合高速识别应用、读写器的发射功率容限、射频标签及读写器的价格等方面。典型的微波射频标签的识读距离为 3～5m，个别有达 10m 或 10m 以上的产品。对于可无线读/写的射频标签而言，通常情况下，写入距离要小于识读距离，其原因在于写入要求更大的能量。

微波射频标签的数据存储容量一般限定在 2KBits 以内，再大的存储容量几乎没有太大的意义，从技术及应用的角度来说，微波射频标签并不适合作为大量数据的载体，其主要功能在于标识物品并完成无接触的识别过程。典型的数据容量指标有：1KBits，128Bits，64Bits 等。由 Auto-ID Center 制定的产品电子代码 EPC 的容量为 90Bits。

微波射频标签的典型应用包括：移动车辆识别、电子身份证、仓储物流应用、电子闭锁防盗（电子遥控门锁控制器）等。相关的国际标准有：ISO10374，ISO18000—4（2.45GHz）、ISO18000—5（5.8GHz）、ISO18000—6（860—930MHz）、ISO18000—7（433.92MHz），ANSI NCITS256—1999 等。

2.2.4　RFID 中间件

RFID 中间件（Middleware）可称为 RFID 运作的中枢，因为它可以加速关键应用的产生。

RFID 产业潜力无穷，应用的范围遍及制造、物流、医疗、运输、零售、国防等。Gartner Group 认为，RFID 是 2005 年建议企业可考虑引入的十大策略技术之一，然而其成功之关键除了标签（Tag）的价格、天线的设计、波段的标准化、设备的认证之外，最重要的是要有关键的应用软件（Killer Application），才能迅速推广。而中间件可称为 RFID 运作的中枢，因为它可以加速关键应用的产生。

1. RFID 的中间件的原理与分类

RFID 中间件是一种面向消息的中间件（Message-Oriented Middleware，MOM），信息（Information）是以消息（Message）的形式，从一个程序传送到另一个或多个程序。信息可以以异步（Asynchronous）的方式传送，所以传送者不必等待回应。面向消息的中间件包含的功能不仅是传递（Passing）信息，还必须包括解译数据、安全性、数据广播、错误恢复、定位网络资源、找出符合成本的路径、消息与要求的优先次序，以及延伸的除错工具等服务。

根据 ABI Research Inc.的预测，2008 年之前全球各产业的需求所创造出来的 RFID 市场规模可达到 200 亿美元，其中软件市场约占 47 亿美元，2007 年 RFID 的整合服务收入将超越 RFID 产品收入。随着硬件技术逐渐成熟，庞大的软件市场商机促使国内外信息服务厂商无不持续关注与提早投入，RFID 中间件在各项 RFID 产业应用中居于神经中枢，特别受到国际大厂的关注，未来在应用上可朝下列方向发展。

（1）面向服务的架构 RFID 中间件

面向服务的架构（Service Oriented Architecture Based，SOA）的目标就是建立沟通标准，突破应用程序对应用程序沟通的障碍，实现商业流程自动化，支持商业模式的创新，让 IT 变得更灵活，从而更快地响应需求。因此，RFID 中间件在未来发展上，将会以面向

服务的架构为基础的趋势，提供企业更弹性灵活的服务。

（2）安全架构（Security Infrastructure）

RFID 应用最让外界质疑的是 RFID 后端系统所连接的大量厂商数据库可能引发的商业信息安全问题，尤其是消费者的信息隐私权。通过大量 RFID 读写器的布置，人类的生活与行为将因 RFID 而容易追踪。Wal Mart、Tesco（英国最大零售商）在 RFID PilotProject 初期就因为用户隐私权问题而遭受过抵制与抗议。为此，飞利浦半导体等厂商已经开始在批量生产的 RFID 芯片上加入“屏蔽”功能。RSA Security 也发布了能成功干扰 RFID 信号的技术——“RSA Blocker 标签”，通过发射无线射频扰乱 RFID 读写器，让 RFID 读写器误以为搜集到的是垃圾信息而错失数据，从而达到保护消费者隐私权的目的。目前 Auto-ID Center 也正在研究安全机制以配合 RFID 中间件的工作。相信安全将是 RFID 未来发展的重点之一，也是成功的关键因素。

2. 分类与发展

（1）RFID 的分类

RFID 中间件可以从架构上分为以下两种。

以应用程序为中心（Application Centric）的设计概念是通过 RFID 读写器（Reader）厂商提供的 API，以热代码（Hot Code）方式直接编写特定读写器（Reader）读取数据的适配器（Adapter），并传送至后端系统的应用程序或数据库，从而达成与后端系统或服务串接的目的。

以架构为中心（Infrastructure Centric）随着企业应用系统的复杂度增高，企业无法负荷以热代码方式为每个应用程式编写适配器，同时面对对象标准化等问题，企业可以考虑采用厂商所提供标准规格的 RFID 中间件。这样一来，即使存储 RFID 标签情报的数据库软件改由其他软件代替，或读写 RFID 标签的 RFID 读写器种类增加等情况发生时，应用端不做修改也能应付。

（2）RFID 中间件的特征

一般来说，RFID 中间件具有以下特点。

1）独立于架构（Insulation Infrastructure）。RFID 中间件独立并介于 RFID 读写器与后端应用程序之间，并且能够与多个 RFID 读写器以及多个后端应用程序连接，以减轻架构与维护的复杂性。

2）数据流（Data Flow）。RFID 的主要目的在于将实体对象转换为信息环境下的虚拟对象，因此数据处理是 RFID 最重要的功能。RFID 中间件具有数据的搜集、过滤、整合与传递等特性，以便将正确的对象信息传到企业后端的应用系统。

3）处理流（Process Flow）。RFID 中间件采用程序逻辑及存储再转送（Store-and-Forward）的功能来提供顺序的消息流，具有数据流设计与管理的能力。

标准（Standard）RFID 为自动数据采样技术与辨识实体对象的应用。EPCglobal 目前正在研究为各种产品的全球唯一识别号码提出通用标准，即 EPC（产品电子编码）。EPC 是在供应链系统中，以一串数字来识别一项特定的商品，通过无线射频辨识标签由 RFID 读写器读入后，传送到计算机或是应用系统中的过程称为对象命名服务（Object Name Service，ONS）。对象命名服务系统会锁定计算机网络中的固定点抓取有关商品的消息。EPC 存放在 RFID 标签中，被 RFID 读写器读出后，即可提供追踪 EPC 所代表的物品名称及相关信息，并立即识别及分享供应链中的物品数据，有效率地提供信息透明度。

RFID 中间件扮演着 RFID 硬件和应用程序之间的中介角色，从应用程序端使用中间件所提供的一组通用应用程序接口（API），即能实现到 RFID 读写器的连接。这样一来，即使存储 RFID 标签数据的数据库软件或后端应用程序增加或改由其他软件取代，或者读/写 RFID 读写器种类增加等情况发生时，应用端不需修改也能处理，解决了多对多连接的维护复杂性问题。RFID 中间件在系统中的作用及位置如图 2-6 所示。

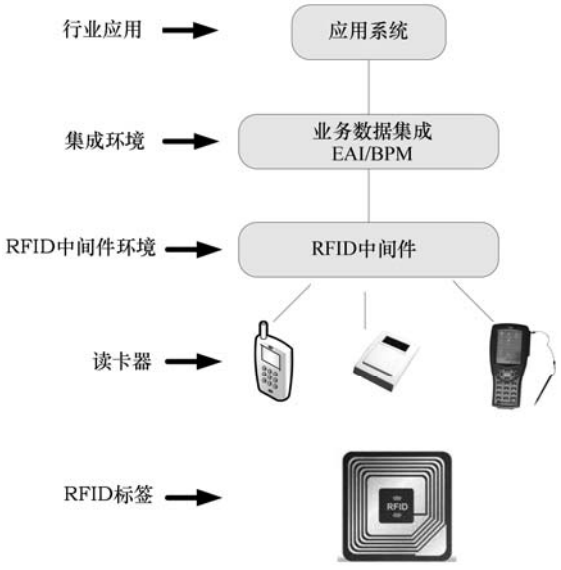


图 2-6　RFID 中间件在系统中的作用及位置

看到目前各式各样 RFID 的应用，企业最想问的第一个问题是：“我要如何将我现有的系统与这些新的 RFID 读写器连接？”这个问题的本质是企业应用系统与硬件接口的问题。因此，通透性是整个应用的关键，正确抓取数据、确保数据读取的可靠性以及有效地将数据传送到后端系统都是必须考虑的问题。传统应用程序与应用程序之间（Application to Application）的数据通透是通过中间件架构解决的，并开发出各种 Application Server 应用软件；同理，中间件的架构设计解决方案便成为 RFID 应用的一项极为重要的核心技术。

（3）RFID 中间件的三大类发展阶段

1）RFID 初期阶段。

RFID 初期的发展多以整合、串接 RFID 读写器为目的，本阶段多为 RFID 读写器厂商主动提供简单 API，以供企业将后端系统与 RFID 读写器串接。以整体发展架构来看，此时企业的导入须自行花费许多成本去处理前后端系统连接的问题，通常企业在本阶段会通过 Pilot Project 方式来评估成本效益与导入的关键议题。

2）架构中间件发展阶段。

本阶段是 RFID 中间件成长的关键阶段。由于 RFID 的强大应用，Wal Mart 与美国国防部等关键使用者相继进行了 RFID 技术的规划并进行导入的 PilotProject，促使各国际大厂持续关注 RFID 相关市场的发展。本阶段 RFID 中间件的发展不但已经具备基本数据搜集、过滤等功能，同时也满足企业多对多（Devices-to-Applications）的连接需求，并具备平台的管理与维护功能。

3）解决方案中间件发展阶段。

未来在 RFID 标签、读写器与中间件发展成熟过程中，各厂商针对不同领域提出各项创新应用解决方案，例如 Manhattan Associates 提出“RFID in a Box”，企业不需再为前端 RFID 硬件与后端应用系统的连接而烦恼，该公司与 Alien TechnologyCorp 在 RFID 硬件端合作，发展 Microsoft. Net 平台为基础的中间件，针对该公司 900 家已有供应链客户群发展 Supply Chain Execution（SCE）Solution，原本使用 Manhattan Associates SCE Solution 的企业只需通过“RFID in a Box”，就可以在原有应用系统上快速利用 RFID 来加强供应链管理的透明度。

3. RFID 内部信息安全与保护

工业标准正在被强化，以保护存储在 RFID 芯片中信息的安全。业界正在为强化相关的工业标准而工作，以保护存储在 RFID 芯片中数据的安全，避免黑客利用 RFID 中存储的敏感信息，进行非法活动，以获得暴利。

2004 年是 RFID 技术发展的关键时期，因为所有相关的技术标准会陆续发布，以满足美国商业巨头沃尔玛和美国国防部等大量物流应用所需。目前制定 RFID 标准的组织比较著名的有三个：ISO、以美国为首的 EPCglobal 以及日本的 Ubiquitous ID Center，而这三个组织对 RFID 技术应用规范都有各自的目标与发展规划。如果从发展的角度来观察全球 RFID 标准制定，目前最为积极的非 EPCglobal 莫属。目前，我国也已经成立了一个 RFID 国家标准工作组，正在制定相关的 RFID 国家标准。

（1）RFID 安全

RFID 数据非常容易受到攻击，主要是 RFID 芯片本身，以及芯片在读或者写数据的过程中都很容易为黑客所利用。在美国 LasVegas 举行的 Black Hat 2004 会议上，Lukas Grunwald

公开展示了一个名为 RFDump 的工具，它可以利用 RFID 系统的弱点发动攻击。任何一个人，只要在自己的便携式计算机中插上一个读卡器，就可以使用 RFDump 软件获得 3 英尺内的被动式 RFID 芯片中的数据。

Counterpane Internet Security 公司的首席技术官 Bruce Schneier 先生对此有自己的看法。他认为，Lukas Grunwald 所做的事情在 RFID 工作中经常会出现，这是一个严肃、认真的工作，他并没有进行任何攻击行动。RFID 在当初的设计中是完全开放的，这是出现安全问题的根本原因。他研究了 RFID 的技术规范、读/写过程和其他问题，发现了其中隐藏的安全问题。假如你对芯片的安全不放心，那么你也会发现这些问题。假如在芯片中有保护措施，任何人也不会轻易就能对 RFID 系统发动攻击。

其实，RFID 标签由耦合元件及芯片组成，每个标签具有唯一的电子编码，附着在物体目标对象上。其封装可以有不同形式，例如常见的信用卡形式及小圆片的形式等。从能量方面来看，标签可以分为两种：无源标签和有源标签。无源标签自身不带有电源，当读取装置对标签进行读取时，所发射出的无线电接触到 RFID 标签的天线后产生能量，它的质量轻、体积小，寿命可以很长，但是发射距离受限。有源标签使用卡内的电池能量，识别的距离长，但是它的价格较高且寿命短。

按调制方式来分，RFID 又分为主动式标签和被动式标签。主动式标签用自身的射频能量主动地给读写器发送数据，主要用于有障碍物的应用中；被动式标签使用调制散射方式发射数据，它必须利用读写器的载波来调制自己的信号，适宜用在门禁或交通的应用中。RFDump 确实是当前所使用的 RFID 芯片的一个巨大威胁。但是按照工业界的一些资料显示，RFID 的这些弱点被发现已经有一段不算短的时间了。一项用于保护 RFID 数据的新标准已经在 2004 年 6 月获得批准，这是 Epcgolbal 发布的第二代 RFID 标准。

根据市场研究公司 IDC 公司的调查，RFID 存储安全隐患并不是阻碍其市场发展的主要因素。位于美国马萨诸塞州的 IDC 研究机构预测：RFID 的市场将从现在的 9150 万美元，增长到 2008 年的 13 亿美元。而非营利组织 EPCglobal 产品管理的负责人 Sue Hutchinson 女士认为，RFID 市场最大的增长来自供应链应用市场，全程监控产品的流动过程，从生产制造，经过运输和仓储，到达零售商和最终的消费者的全过程。EPCglobal 是一家总部位于美国新泽西州 Lawrenceville 的负责电子产品代码标准制定与应用的工业贸易组织。

（2）第二代 RFID 的安全功能

第二代 RFID 标准针对供应链应用，最终用户提出了一系列需求，这些成为制定第二代 RFID 标准的重要基础。开发中最主要的部分是设计了第二代的 UHF（超高频率）空中接口协议，该协议用于管理从标签到读卡器的数据的移动，为芯片中存储的数据提供了一些保护措施。新标准采用了一个安全的链路，保护被动标签免于受诸如 RFDump 和其他一些在供应链应用中被发现的大多数攻击行为。当数据被写入标签时，数据在经过空中接口

时被伪装。从标签到读卡器的所有数据都被伪装，所以当读卡器在从标签读或者写数据时数据不会被截取。一旦数据被写入标签，数据就会被锁定，这样只可以读取数据，而不能被改写，就是具有我们常说的只读功能。

EPC 被动标签一般只包括产品的识别信息，比如产品代码、产品部件数，或者 SKU 数目，也就是仅仅包括物品本身的信息。EPC 被动标签不包括依据秘密保护规则涉及的物品个性化的识别信息。产品的识别信息通常是指相对于个性化识别信息而言不太敏感的内容，通常伪装也只针对其中涉及的数据。数据并不被加密，但是读卡器需要一个破解伪装的“密钥”。美国国防部公布了其最终的针对供应链应用的 RFID 规范，其中并没有包括数据加密要求。Estevez 先生列举了两条理由，说明 DOD 规范的合理性：第一，产品信息比如序列号等在它没有被整合到带有附加信息的数据库之前，并没有太多值得利用的信息；第二，潜在的“敌人”不可能非常近距离地接近它，比如在 10 英尺之内，以读取标签上的信息。

（3）金融领域 RFID 的安全

当 RFID 包括了消费者的相关数据时，供应链 RFID 应用可能才会真正走向成熟。Hutchinson 认为，EPCglobal 未来的一项主要任务就是制定包含用户数据的更高级别的 RFID 标签工业标准。因此，会更关注 RFID 的安全问题，也包括减少每年全球在供应链方面 1800 亿～3000 亿美元的损失。这一数据是美国零售业领导协会（Retail Industry Leaders Association）估计的。

RFID 标签从功能方面来看分为四种：只读标签、可重写标签、带微处理器标签和配有传感器的标签。只读型标签的结构功能最简单，包含的信息较少并且不能被更改；可重写型标签集成了容量为几十字节到几万字节的闪存，标签内的信息能被更改或重写，只读型和可重写型 RFID 标签都主要应用于物流系统以及生产过程管理系统和行李控制系统中；带微处理器标签依靠内置式只读存储器中存储的操作系统和程序来工作，出于安全的需要，许多标签都同时具备加密电路，现在这类标签主要应用于非接触型 IC 卡上，既用于电子结算、出入管理，也可用于会员卡；有些 RFID 标签集成了传感器，包括温度传感器或压力传感器等，目前这类标签主要用于动物个体识别和轮胎管理方面。银行业和电子支付卡行业在保护存储在 RFID 卡上的个人识别信息方面更有实践经验，Visa 和电子支付卡行业更愿意选择 EMV 卡。EMV 规范系国际三大著名银行卡组织（Visa、MASTERCARD、EUROPAY）联合制定的金融 IC 卡业界标准，在金融 IC 卡领域具有最高权威性，EMV 规范的实施对于成员国银行改善在国际化过程中的银行卡受理环境、降低在国际商务应用中的信用卡风险等方面起着举足轻重的作用。为保证我国 IC 卡的国际通用性和国外银行卡在我国的通用性，我国目前正在进行银行卡 EMV 标准的迁移，并着手修订与之相对应的国内金融 IC 卡的 PBOC 标准。

最新的非接触 EMV 卡遵守 ISO14443 标准卡的规定，它可以在 10cm 的范围内被各种

设备读取。它们可以依照被每一个遵守标准国家的每一个发卡银行认可的保密和安全的标准进行配置。银行卡上实际加密的部分是一个卡识别一个经过授权的读卡器的部分，以应对日益严峻的挑战。加密的其余部分是在银行的后端系统处理。这是一个在全球所有的国家都能正常工作的全球范围的系统，它使用一种所有银行都采用的加密技术，可以对多种不同的数据进行加密。

2.2.5　RFID 与条码的比较

从概念上来说，RFID 与条码两者很相似，目的都是快速准确地确认追踪目标物体。但它们作为两种不同的技术，RFID 对比条形码还是有着自身的许多优点。

1）快速扫描。条形码一次只能有一个条形码受到扫描；RFID 辨识器可同时辨识并读取数个 RFID 标签。

2）体积小型化、形状多样化。RFID 在读取上不受尺寸大小与形状限制，不需为了读取精确度而配合纸张的固定尺寸和印制品质。此外，RFID 标签更可往小型化与多样形态发展，以应用于不同产品。

3）不要求看见目标。两者之间最大的区别是，条形码是“可视技术”，扫描仪在人的指导下工作，只能接收它视野范围内的条形码。相比之下，RFID 不要求看见目标。RFID 只要在接收器的作用范围内就可以被读取。

4）抗污染能力和耐久性。传统条形码的载体是纸张，因此容易受到污损，但 RFID 对水、油和化学药品等物质具有很强的抵抗性。此外，由于条形码是附着在塑料袋或外包装纸箱上，所以特别容易受到折损；RFID 卷标是将数据存在芯片中，因此可以免受污损。

5）可重复使用。现今的条形码印制上去之后就无法更改，RFID 标签则可以重复地新增、修改、删除 RFID 卷标内储存的数据，方便信息的更新。

6）穿透性和无屏障阅读。在被覆盖的情况下，RFID 能够穿透纸张、木材和塑料等非金属或非透明的材质，并能够进行穿透性通信。而条形码扫描机必须在近距离而且没有物体阻挡的情况下，才可以辨读条形码。

7）数据的记忆容量大。一维条形码的容量是 50B，二维条形码最大的容量可储存 2～3000 字符，RFID 最大的容量则有数 MB。随着记忆载体的发展，数据容量也有不断扩大的趋势。未来物品所需携带的资料量会越来越大，对卷标所能扩充容量的需求也相应增加。

8）安全性。由于 RFID 承载的是电子式信息，其数据内容可经由密码保护，使其内容不易被伪造及变造。但目前来说，RFID 标签还不能完全取代条码技术，这也是由很多因素决定的。

自 20 世纪 70 年代以来，条码技术一直是商品清单管理的主流方法。一个条码的价格

不到 0.01 美元，并且还有统一的管理标准，推动了零售业的革命化与商品的物流管理。与条码技术相比，RFID 标签识别技术更有特点，解决了有些条件下条码等其他识别技术无法使用的问题，并开拓了许多新的应用领域。但由于其价格高于条码，且缺乏统一的标准等原因，尽管不少业内人士认为 RFID 标签将成为“下一代的条码”，但在相当长的时间内，RFID 标签还将与条码技术并存。

RFID 的标准化问题。条码自动识别技术，在许多行业中都有共同的标准，并且已有多年的实践传统。RFID 技术不像条码，目前还缺乏统一的标准。虽有常用的共同频率范围，但制造厂商可以自行改变。此外，标签上的芯片性能、存储器存储协议与天线设计约定等，也都没有统一标准。尽管 RFID 的有关标准正在逐步开发制定、不断完善，但是不同国家又有自己的规则。有的业内人士担心，比制定条码标准更为困难的是，如果一个国家把某个频率权卖给某个商业企业后，在出现对其他系统的干扰时，这个国家就很难对这个频率段的使用情况进行监督管理。

由于制造技术较为复杂，生产费用相应较高，在新的制造工艺没有普及推广之前，高成本的 RFID 标签只能用于一些本身价值较高的产品。美国目前一个 RFID 标签的价格为 0.30～0.60 美元，对比较贵重或高档的产品来说，0.50 美元左右的价格还比较容易被厂商接受，在这些厂商看来，RFID 标签是一个优秀的识别跟踪装置。当然，对一些价位较低的商品，如果采用高档 RFID 标签显然有些不划算了。不过，随着新的 RFID 标签制造技术的推广应用，将会促使 RFID 标签价格大幅度降低，RFID 标签必将得到更广泛的应用。

据介绍，有些研究单位正在利用 RFID 技术创制新的通用、开放的网络和相应的标准，当产品在全球供应链流通时，通过标签能对产品进行跟踪。例如，美国 MIT 高等学府的 Auto-ID Center（自动化识别中心）正在开发包括标签、读写器与计算机组合的 Electronic Product Code（EPC）网络，能使制造商与零售商实现实时跟踪，进行准确的商品库存管理，其关键技术就是采用了 RFID 标签。这类新型的跟踪管理网络技术的推出使条码技术的应用前景变得十分暗淡。

然而，这些研发单位的初衷并不是要取代条码。Auto-ID Center 并不主张完全用该技术代替条码，因为基于条码的系统已成为许多行业标准的自动化识别技术，并且已有多年的应用历史。为 RFID 标签生产导电油墨的 Flint Ink 公司认为：与条码相比，RFID 标签的价格显得略高，因此，条码仍然会继续使用若干年。虽然 RFID 技术被认为是“下一代的条码”，但现在正在大量使用的条码不可能很快被取代。许多观察家预言，RFID 将与条码并存，两种技术各有特点。在许多情况下，需要根据具体情况来确定是采用 RFID 技术还是采用条码技术，以满足不同的使用要求。

2.2.6　RFID 系统设计中的注意事项

（1）工作方式选取

射频识别系统的基本工作方式分为全双工（Full Duplex）和半双工（Half Duplex）系统以及时序（SEQ）系统。全双工表示射频标签与读写器之间可在同一时刻互相传送信息。半双工表示射频标签与读写器之间可以双向传送信息，但在同一时刻只能向一个方向传送信息。

在全双工和半双工系统中，射频标签的响应是在读写器发出的电磁场或电磁波的情况下发送出去的。因为与阅读器本身的信号相比，射频标签的信号在接收天线上是很弱的，所以必须使用合适的传输方法，以便把射频标签的信号与阅读器的信号区别开来。在实践中，人们对从射频标签到阅读器的数据传输一般采用负载反射调制技术将射频标签数据加载到反射回波上（尤其是针对无源射频标签系统）。

时序方法则与之相反，阅读器辐射出的电磁场短时间周期性地断开。这些间隔被射频标签识别出来，并被用于从射频标签到阅读器的数据传输。其实，这是一种典型的雷达工作方式。时序方法的缺点是：在阅读器发送间歇时，射频标签的能量供应中断，这就必须通过装入足够大的辅助电容器或辅助电池进行补偿。

（2）数据量

射频识别射频标签的数据量通常在几个字节到几千个字节之间。但是，有一个例外，这就是 1Bit 射频标签。它有 1Bit 的数据量就足够了，使阅读器能够做出以下两种状态的判断：“在电磁场中有射频标签”或“在电磁场中无射频标签”。这种要求对于实现简单的监控或信号发送功能是完全足够的。因为 1Bit 的射频标签不需要电子芯片，所以射频标签的成本可以做得很低。由于这个原因，大量的 1Bit 射频标签在百货商场和商店中用于商品防盗系统（EAS）。当带着没有付款的商品离开百货商场时，安装在出口的读写器就能识别出“在电磁场中有射频标签”的状况，并引起相应的反应。对按规定已付款的商品来说，1Bit 射频标签在付款处被除掉或者去活化。

（3）可编程

能否给射频标签写入数据是区分射频识别系统的另外一个因素。对简单的射频识别系统来说，射频标签的数据大多是简单的（序列）号码，可在加工芯片时集成进去，以后不能再变。与此相反，可写入的射频标签通过读写器或专用的编程设备写入数据。

射频标签的数据写入一般分为无线写入与有线写入两种形式。目前铁路应用的机车、货车射频标签均采用有线写入的工作方式。

（4）数据载体

为了存储数据，主要使用三种方法：EEPROM、FRAM、SRAM。对一般的射频识别

系统来说，使用电可擦可编程只读存储器（EEPROM）是主要方法。然而，使用这种方法的缺点是：写入过程中的功率消耗很大，使用寿命一般为写入 100000 次。最近，也有个别厂家使用所谓的铁电随机存取存储器（FRAM）。与电可擦可编程只读存储器相比，铁电随机存取存储器的写入功率消耗减小到原来的百分之一，写入时间甚至减小到原来的千分之一。然而，铁电随机存取存储器由于生产中的问题至今未获得广泛应用。FRAM 属于非易失类存储器。

对微波系统来说，还使用静态随机存取存储器（SRAM），存储器能很快写入数据。为了永久保存数据，需要用辅助电池做不中断的供电。

（5）状态模式

对可编程射频标签来说，必须由数据载体的“内部逻辑”控制对标签存储器的写/读操作以及对写/读授权的请求。在最简单的情况下，可由一台状态机来完成。使用状态机可以完成很复杂的过程。然而，状态机的缺点是：对修改编程的功能缺乏灵活性，这意味着要设计新的芯片，由于这些变化需要修改硅芯片上的电路，设计更改实现所要的花费很大。

微处理器的使用明显地改善了这种情况。在芯片生产时，将用于管理应用数据的操作系统，通过掩膜方式集成到微处理器中，这种修改花费不多。此外，软件还能调整以适合各种专门应用。

此外，还有利用各种物理效应存储数据的射频标签，其中包括只读的表面波（SAW）射频标签和通常能去活化（写入“0”）以及极少的可以重新活化（写入“1”）的 1Bit 射频标签。

（6）能量供应

射频识别系统的一个重要的特征是射频标签的供电。无源的射频标签自己没有电源。因此，无源的射频标签工作用的所有能量必须从阅读器发出的电磁场中取得。与此相反，有源的射频标签包含一个电池，为微型芯片的工作提供全部或部分（辅助电池）能量。

（7）频率范围

射频识别系统的另一个重要特征是系统的工作频率和阅读距离。可以说工作频率与阅读距离是密切相关的，这是由电磁波的传播特性所决定的。通常把射频识别系统的工作频率定义为阅读器读射频标签时发送射频信号所使用的频率。在大多数情况下，把它称为阅读器发送频率（负载调制、反向散射）。不管在何种情况下，射频标签的“发射功率”要比阅读器发射功率低很多。

射频识别系统阅读器发送的频率基本上划归三个范围：

1）低频（30～300kHz）。

2）中高频（3～30MHz）。

3）超高频（300MHz～3GHz）或微波（>3GHz）。

根据作用距离，射频识别系统的附加分类是：密耦合（0～1cm）、遥耦合（0～1m）和远距离系统（>1m）。

（8）射频标签→读写器数据传输

射频标签回送到阅读器的数据传输方式多种多样，可归结为三类：

1）利用负载调制的反射或反向散射方式（反射波的频率与阅读器的发送频率一致）。

2）利用阅读器发送频率的次谐波传送标签信息［标签反射波与阅读器的发送频率不同，为其高次谐波（n 倍）或分谐波（1/n 倍）］。

3）其他形式。

2.2.7　射频技术典型应用

射频识别技术以其独特的优势，逐渐被广泛应用于工业自动化、商业自动化和交通运输控制管理等领域。随着大型集成电路技术的进步以及生产规模的不断扩大，射频识别产品的成本将不断降低，其应用将越来越广泛。表 2-3 列举了射频识别技术几个典型的应用。

表 2-3　射频识别技术的典型应用

典型应用领域	具体应用内容
车辆自动识别管理	铁路车号自动识别是射频识别技术最普遍的应用
高速公路收费及智能交通系统	高速公路自动收费系统是射频识别技术最成功的应用之一，它充分体现了非接触识别的优势。在车辆高速通过收费站的同时完成缴费，解决了交通的瓶颈问题，提高了车行速度，避免拥堵，提高了收费结算效率
货物的跟踪、管理及监控	射频识别技术为货物的跟踪、管理及监控提供了便捷、准确、自动化的手段。以射频识别技术为核心的集装箱自动识别，成为全球范围最大的货物跟踪管理应用
仓储、配送等物流环节	随着射频识别技术在开放的物流环节统一标准的研究开发，物流业将成为射频识别技术最大的受益行业
电子钱包、电子票证	射频识别卡的功能相当于电子钱包，实现非现金结算。目前主要应用在交通方面
生产线产品加工过程自动控制	在大型工厂的自动化流水作业线上，实现自动控制、监视，提高生产效率，节约成本
动物跟踪和管理	在大型养殖场，可通过采用射频识别技术建立饲养档案、预防接种档案等，达到高效、自动化管理牲畜的目的，同时为食品安全提供了保障。射频识别技术还可用于信鸽比赛、赛马识别等，以准确测定到达时间

2.2.8 RFID 遇到的挑战

RFID 在推广应用中遇到了不少挑战，主要表现在成本、标准、精确度与应用模式等方面。即缺乏成熟的应用模式和行业标准，以及相关产品标准不统一。

（1）标准化是个大问题

标准化是推动产品广泛获得市场接受的必要措施，但射频识别读取器与标签的技术仍未统一，因此无法一体化使用。不同制造商所开发的标签通信协定，使用不同频率，且封包格式不一。而 RFID 技术不像条码，虽有常用的共同频率范围，但制造厂商可以自行改变，此外，标签上的芯片性能、存储器存储协议与天线设计约定等，也都没有统一标准。尽管 RFID 的有关标准正在逐步开发制定，不断完善，但是不同国家又有自己的规则。有的业内人士担心，比制定条码标准各国更为困难的是，如果一个国家把某个频率权卖给某个商业企业后，在出现对其他系统的干扰时，这个国家就很难对这个频率段的使用情况进行监督管理。

（2）价格问题

价格问题是制约 RFID 标签推广应用市场发展的巨大瓶颈之一。RFID 系统不论是标签、读取器和天线，其价格都比较昂贵。在新的制造工艺没有普及推广之前，高成本的 RFID 标签只能用于一些本身价值较高的产品。美国目前一个 RFID 标签的价格约为 0.30～0.60 美元，对一些价位较低商品，采用高档 RFID 标签显然不划算。另外，对使用 RFID 系统客户而言，其设备投资也不菲，据有关报告指出，为每个商店安装一台 RFID 和 EPC（电子产品编码）识读装置的成本至少是 10 万美元，对一个组织而言，这方面的投资可能会达到 3000～4000 美元。

（3）技术的突破

RFID 技术上尚未完全成熟，特别是应用于某些特殊的产品，如液体或金属罐等时，大量 RFID 标签无法正常起作用。标签的可靠性也是个大问题。就目前看来，现在普遍使用的 134kHz 和 13.56kHz 频率因传输距离太短，限制了阅读器和 RFID 标签间的传输距离，使若干标签不能有效地被读取，标签失效率很高。此外，RFID 标签与读取器有方向性，射频识别信号易被物体阻断，也是 RFID 技术发展一大挑战。即使贴上双重标签，仍有 3%的标签无法识别。

（4）涉及人员失业、隐私保护以及安全问题

企业采用射频识别系统后，原来由手工完成的工作将有很多被该系统取代，其衍生而来的问题就是将有许多劳工面临失去工作的危机。同时 RFID 的大规模应用还会涉及隐私保护以及安全问题，当前的无源 RFID 系统没有读/写能力，所以无法使用密钥验证方法来进行身份验证，如果标签是有源的，并且会收到不断变化的验证密钥，那将会大大提高其

安全性，不过这又会增加其成本。正因为如此，目前的 RFID 技术要想在对信息有保密要求的领域展开应用还存在着一定的障碍。

2.3 中间件

中间件是一类连接软件组件和应用的计算机软件，它包括一组服务，以便于运行在一台或多台机器上的多个软件通过网络进行交互。该技术所提供的互操作性，推动了一致分布式体系架构的演进。该架构通常用于支持分布式应用程序并简化其复杂度，它包括 Web 服务器、事务监控器和消息队列软件。中间件与各相关件之间的关系如图 2-7 所示。

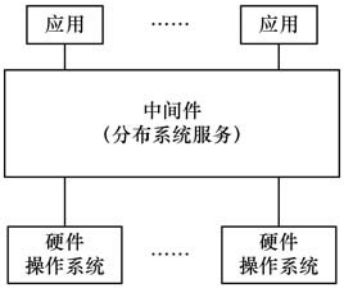


图 2-7　中间件与各相关件之间的关系

2.3.1 中间件分类

中间件的概念产生以来一直没有统一而标准的定义，一直在发展中不断地补充其内涵。由于包括的内容较多，对于不同的需求出现多种产品使得表述起来更加复杂。

从应用和系统角度来看，中间件概念的作用在于屏蔽了底层操作系统的复杂性，可使软件开发人员在简单而统一的开发环境下，着力应用对象特点的开发工作上，不要重复已有可利用的内容，只要完成特殊的内容，这不仅降低了大程序设计的复杂性，而且提高了工作的效率，同时减少了系统的维护、运行和管理的工作量，还减少了其他相关的费用。由于中间件作为新层次的基础软件，其重要作用是将不同时期、在不同操作系统上开发的应用软件集成起来，彼此整体协调工作。只能根据在系统中所起的作用和采用的技术不同来对其进行表述，通常可分为以下几类。

（1）数据访问中间件

数据访问中间件是系统中建立数据应用资源互操作的一种模式。在异构环境下的数据库连接或文件系统连接，为在网络中虚拟缓冲存取、格式转换、解压等带来方便。数据访

问中间件在所有的中间件中是应用最广泛、技术最成熟的一种。这种方式虽然灵活，但是并不适合一些要求高性能处理的场合，因为其中需要进行大量的数据通信，而且当网络发生故障时，系统将不能正常工作。

（2）远程调用中间件（RPCM）

远程调用中间件是一种广泛使用的分布式应用程序处理方法，是用于执行一个位于不同地址空间里的过程。当一个应用程序 A 需要与远程的另一个应用程序 B 交换信息或要求 B 提供协助时，A 在本地产生一个请求，通过通信链路通知 B 接收信息或提供相应的服务，B 完成相关处理后将信息或结果返回给 A。

PRCM 在客户服务器计算方面，比数据访问中间件又迈进了一步。在 RPC 模型中，客户机和服务器只要具备了相应的 RPC 接口，并且具有 RPC 运行支持，就可以完成相应的互操作，而不必限制于特定的服务器。远程过程调用（RPC）所提供的是基于过程的服务访问，客户/服务器进行直接连接，没有中间机构来处理请求，因此也具有一定的局限性。比如：RPC 通常需要一些网络细节以定位服务器；在客户端发出请求的同时，要求服务器必须处于工作状态；等等。

（3）面向对象的中间件

面向对象中间件（OOM）将编程模型从面向过程升级为面向对象，对象之间的方法调用通过对象请求代理（ORB）转发。ORB 能够为应用提供位置透明性和平台无关性，接口定义语言（IDL）还可能提供语言无关性。该类中间件还为分布式应用环境提供多种基本服务，如名录服务、事件服务、生命周期服务、安全服务和事务服务等。这类中间件的代表有 CORBA、DCOM、JavaRMI。

（4）基于事件的中间件（EBM）

大规模分布式系统拥有数量众多的用户和联网设备，没有中心控制点，系统需对环境、信息和进程状态的变化做出响应。此时传统的一对一请求/应答模式已不再适合，而基于事件的系统以事件作为主要交互手段，允许对象之间异步、对等的交互，特别适合广域分布式系统对松散、异步交互模式的要求。基于事件的中间件关注为建立基于事件的系统所需的服务和组件的概念、设计、实现和应用问题。它提供了面向事件的编程模型，支持异步通信机制，与面向对象的中间件相比有更好的可扩展性。

（5）面向消息的中间件（MOM）

面向消息的中间件是基于报文传递的网络通信机制的自然延伸，其工作方式类似于电子邮件：发送方只负责消息的发送，消息内容由接收方解释并采取相应的行动；消息暂存在消息队列中，若需要可在任何时候取出，通信双方不需要同时在线。它利用高效、可靠的消息传递机制进行与平台无关的数据交流，并基于数据通信实现分布式系统的集成。通过提供消息传递和消息排队模型，可在分布环境下扩展进程间的通信，并支持多通信协议、

语言、应用程序、硬件和软件平台。由于没有同步建立过程，也不需要对调用参数进行编码/解码，所以消息中间件效率较高，而且有更强的可扩展性和灵活性，更适合建立企业级或跨企业的大规模分布式系统。但消息中间件的异步通信方式可能不适合有实时要求的应用。另外从编程的角度看，其抽象级别较低，容易出错，不易调试，因此消息中间件可看成实际需求和抽象等级间的一种折中。消息中间件通常有消息传递/消息队列和出版/订阅两种类型。在交互模式上，前者是“推”模式，后者是“拉”模式。典型的面向消息的中间件产品有 BEA 的消息 Q、微软的 MSMQ、IBM 的消息排队系统 MQ 系列。消息传递和排队技术主要有以下三个特点：

1）通信程序可在不同的时间运行。程序不在网络上直接相互通话，而是间接地将消息放入消息队列，程序间没有直接的联系，也不必同时运行。当消息放入适当的队列时，目标程序甚至根本不需要在运行之中；即使目标程序在运行，也不意味着要立即处理该消息。

2）对应用程序的结构没有约束。在复杂的应用场合中，通信程序之间不仅可以是一对一的关系，还可以进行一对多和多对一方式，甚至是上述多种方式的组合。多种通信方式的构造并没有增加应用程序的复杂性。

3）程序与网络复杂性相隔离。程序将消息放入消息队列或从消息队列中取出来实现相互之间的通信，与此关联的全部活动（比如维护消息队列、维护程序和队列之间的关系、处理网络的重新启动和在网络中移动消息等）是 MOM 的任务，程序不直接与其他程序通话，且不涉及网络通信的复杂性。

（6）面向对象代理的中间件

随着面向对象技术与分布式计算技术的发展，两者相互结合形成了分布对象计算，并发展为当今软件技术的主流方向。1990 年年底，对象管理集团（OMG）首次推出对象管理结构（OMA），对象请求代理（ORB）是其中的核心组件。它的作用在于提供一个通信框架，定义异构环境下对象透明地发送请求和接收响应的基本机制，建立对象之间的关系。

ORB 使得客户机/服务器对象可以透明地向其他对象发出请求或接收其他对象的响应，这些对象可以位于本地也可以位于远程机器。ORB 拦截请求调用，并负责找到可以实现请求的对象、传送参数、调用相应的方法、返回结果等客户端对象并不知道同服务器对象通信、激活或存储、服务器对象的机制，也不必知道服务器对象位于何处、用何种语言、使用什么操作系统或其他不属于对象接口的系统成分。值得指出的是，用户端和服务器的角色只是用来协调对象之间的相互作用，根据相应的场合，ORB 上的对象可以是客户端，也可以是服务器，甚至两者兼而有之。当对象发出一个请求时，它是处于客户端角色；当它在接收请求时，它就处于服务器角色。另外，由于 ORB 负责对象请求的传送和服务器的管理，客户端和服务器之间并不直接连接，因此与 RPC 所支持的单纯客户端和服务器结构相比，ORB 可以支持更加复杂的结构。

（7）事务处理监控中间件

事务处理中间件又称为事务处理监控器（TPM），它支持分布式组件的事务处理，通常有请求队列、会话事务、工作流等模式，可视为事务处理应用程序的“操作系统”。多数事务监控器支持负载均衡和服务组件的管理，具有事务的分布式两阶段提交、安全认证和故障恢复等功能。事务处理监控最早出现在大型机上，为其提供支持大规模事务处理的可靠运行环境。其一方面通过复用和路由技术协调大量客户对服务器的访问，提高系统的可扩展性；另一方面扩展了数据库管理系统的事务处理概念，在各个子系统之间协调全局事务的处理。分布应用系统对大规模的事务处理提出了需求，比如商业活动中大量的关键事务处理。事务处理监控介于客户端和服务器之间，进行事务管理与协调、负载平衡、失败恢复等，以提高系统的整体性能。事务处理监控主要有进程管理、事务管理以及通信管理等功能。

1）进程管理包括启动服务器进程，为其分配任务，监控其执行并对负载进行平衡。

2）事务管理保证在其监控下的事务处理的原则性、一致性、独立性和持久性。

3）通信管理为客户端和服务器之间提供了多种通信机制，包括请求响应、会话、排队、订阅发布和广播等。

事务处理监控能够为大量的客户端提供服务，如飞机订票系统。如果服务器为每一个客户端都分配其所需的资源，在同一时刻并不是所有的客户端都需要请求服务，而一旦某个客户端请求了服务，它希望得到快速的响应。事务处理监控在操作系统之上提供一组服务，对客户端请求进行管理并为其分配相应的服务进程，使服务器在有限的系统资源下能够高效地为大规模的客户群提供服务。

中间件能够屏蔽操作系统和网络协议的差异，为应用程序提供多种通信机制，并提供相应的平台以满足不同领域的需要。因此，中间件为应用程序提供了一个相对稳定的高层应用环境，中间件所应遵循的一些原则离实际还有很大距离。多数流行的中间件服务使用专有的 API 和专有的协议，使得应用建立于单一厂家的产品，来自不同厂家的实现很难互操作。有些中间件服务只提供一些平台的实现，从而限制了应用在异构系统之间的移植。应用开发者在这些中间件服务之上建立自己的应用还要承担相当大的风险，随着技术的发展往往还需重新设计它们的系统。尽管中间件服务提高了分布式计算的抽象化程度，但应用开发者还需要面临许多艰难的设计选择。例如，开发者需决定分布式应用在客户端方和服务器方的功能分配。

2.3.2 中间件基本结构

从应用程序端使用中间件所提供的一组通用的应用程序接口（APl）能够连接到 RFID 读写器，读取 RFID 标签数据。即使存储 RFID 标签信息的数据库软件或后端应用程序增加或由其他软件取代，或者 RFID 读写器种类增加等情况发生，应用端不需要修改也能处理，

从而简化了维护工作。通常选用物联网中间件可以为企业带来几个方面的好处：实施 RFID 项目的企业，不需要进行程序代码开发，便可完成 RFID 数据的导入，可极大地缩短企业 RFID 项目的实施周期；当企业数据库或企业的应用系统发生更改时，对于 RFID 项目而言，只需更改物联网中间件的相关设置即可实现 RFID 数据导入新的企业应用系统；物联网中间件可为企业提供灵活多变的配置操作，企业可以根据自己的实际业务需求和企业应用系统管理的实际情况，自行设定相关的物联网中间件参数，将所需的 RFID 数据顺利地导入企业系统；当 RFID 项目的规模扩大时，例如增加 RFID 读写器数量，更换其他类型的读写器或新增企业仓库，对于使用物联网中间件的企业来说，只需对物联网中间件进行相应的设置，便可完成 RFID 数据的顺利导入，而不需要程序代码的开发。

中间件的体系框架对于应用软件开发有着重要影响，而物联网中的应用软件及中间件，远比操作系统和网络服务更为重要。因为中间件提供的程序接口定义了一个相对稳定的高层应用环境，不管底层的计算机硬件和系统软件怎样更新换代，只要将中间件升级更新，并保持中间件对外的接口定义不变，应用软件几乎无须进行任何修改，从而保护了企业在应用软件开发和维护中的大量投资。由图 2-8 所示的中间件体系结构框架可以看出，中间件应该具备两个关键特征：一个是上层的应用服务；另一个是必须连接到操作系统的层面，并且保持运行工作状态。除了这两个关键特征之外，中间件还有：满足大量应用的需要；运行于多种硬件和操作系统平台；支持分布式计算，提供跨网络、硬件和操作系统平台的透明性的应用或服务的交互；支持标准的协议；支持标准的接口等功能。中间件在物联网的作用和位置如图 2-9 所示。

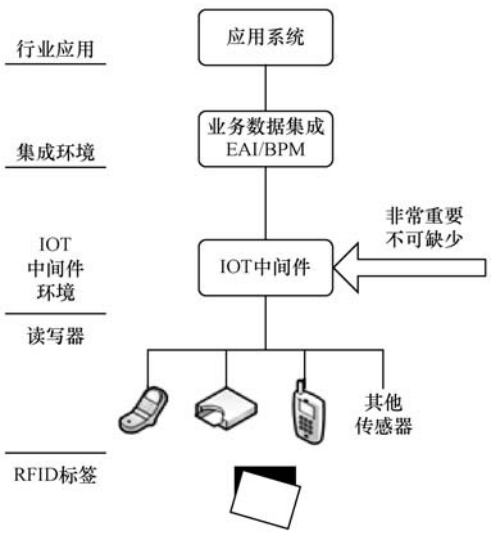


图 2-8　中间件体系结构

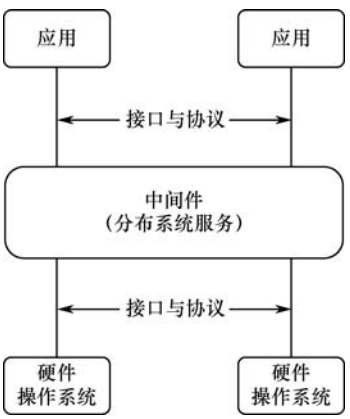


图 2-9　中间件在物联网的作用和位置

中间件的核心模块主要包括事件管理系统（EMS）、实时内存事件数据库（RIED）以及任务管理系统（TMS）三个主要模块。

（1）事件管理系统（EMS）

EMS 配置在“边缘 EPC 中间件”端，用于收集所读到的标签信息。EMS 的主要任务：

1）能够让不同类型的读写器将信息写入到适配器。

2）从读写器中收集标准格式的 EPC 数据。

3）允许过滤器对数据 EPC 数据进行平滑处理。

4）允许将处理后的数据写入 RIED 或数据库，或者通过 HTTP/JMS/SOAP 将 EPC 数据广播到远程服务器。

5）对事件进行缓冲，使得数据记录器（Logger）、数据过滤器（Filter）和适配器（Adapter）能够互不干扰地相互工作。

当事件产生并传递给适配器后，它们将被传递到一个队列，在这个队列中，事件将自动转寄到过滤器，根据不同的过滤器定义，将会有不同的事件被过滤出来。例如，时间过滤器只允许特定时间标记的事件通过。数据记录器与过滤器功能类似，只是记录器主要用于将事件存储到数据库或者将事件传递到某种网络连接。

（2）实时内存事件数据库（RIED）

RIED 是用来存储“边缘 EPC 中间件”事件信息的内存数据库，其中“边缘 EPC 中间件”维护来自读写器的信息，提供过滤和记录事件的框架。

RIED 组件由以下几方面构成：

1）JDBC 接口。JDBC 接口使远程的机器能够使用标准的 SQL 查询语句访问 RIED，并能够使用标准的 URL 定位 RIED。

2）DML 剖析器。DML 剖析器剖析 SQL 数据修改语言，包括标准 SQL 的 SELECT、INSERT 和 UPDATE 命令。RIED 的 DML 剖析器是整个 SQL92DML 规范的子集。

3）查询优化器。查询优化器使用 DML 剖析器的输出，并将其转化为 RIED 可以查询的执行计划，计划定义中定义的搜索路径用来找到一个有效的执行计划。

4）本地查询处理器。本地查询接口处理直接来自应用程序（或者 SQL 剖析器）的执行计划。

5）排序区。排序区是本地查询处理器用来执行排序、分组和连接操作的，排序区使用哈希表来进行连接和分组操作，它使用一种很有效的排序算法来做排序操作。

6）数据结构。RIED 采用线程同步技术，确保多个线程对共享资源进行互斥访问。存储不同的数据快照，这个持久数据结构允许持续创建新的数据快照。这样的数据结构在 RII 的实时操作中是必需的。

7）DDL 剖析器。DDL 剖析器处理计划定义文档和初始化内存模型中的不同数据结构，DDL 剖析器还提供查找定义在 DDL 中的查询路径的功能。

8）回滚缓冲。在 REED 中执行的事务可提交或者回滚，回滚缓冲持有所有的更新直到事务被提交。

（3）任务管理系统（TMS）

物联网中间件系统使用定制的任务来执行数据管理和数据监控。通常一个任务可看作多任务系统的一个过程，EPC 中间件的 TMS 管理任务的方法恰似操作系统管理方法。同时，TMS 提供一些任务操作系统不能提供的特性，如具有时间段任务的外部接口，从冗余的类服务器中随机选择加载 Java 虚拟机的统一类库，强大的调度程序维护任务的持久化信息，能够在 EPC 中间件瘫痪或者任务瘫痪以后重新启动任务。

中间件的 TMS 简化了分布式 EPC 中间件的维护，企业可以通过仅仅保证一系列的类服务器上的任务更新，并更新相关的 EPC 中间件上的调度任务就可以维护 EPC 中间件了。但是，硬件和核心的软件（如操作系统和 Java 虚拟机）必须定期更新。为了 TMS 编写的任务可以访问所有 EPC 中间件的工具。TMS 的任务可以执行各式各样的企业操作，例如：数据收集、发送或者接收另一个 EPC 中间件的产品信息；XML 查询，查询 ONS/XML 服务器手机动态/静态产品实例信息；远程任务调度，调度或者删除另外一个 EPC 中间件上的任务；在一些定义的事件（货架缺货，盗窃，产品过期）发生时，向相关职员发送警告；远程更新，发送产品信息给远程的供应链管理系统。EPC 中间件 TMS 的体系架构如图 2-10 所示。在 TMS 系统中有如下组件：任务管理器、SOAP 服务器、类服务器、数据库。

1）任务管理器。TMS 主要代表用户负责执行和维护运行在 EPC 中间件上的任务，每个提交给系统的任务都有一个时间表，时间表中表明任务的运行周期，是否连续执行等。基于任务的特点和与任务相关的时间表，定义如下任务类型。

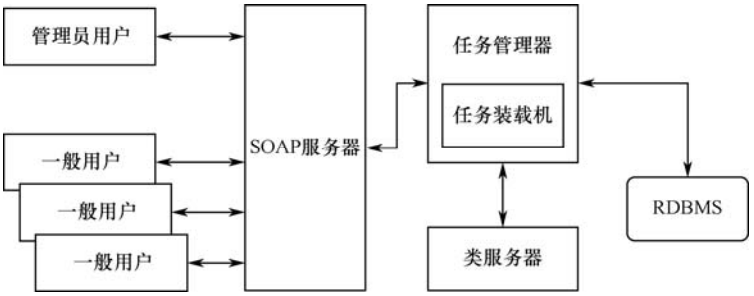


图 2-10　TMS 体系架构

一次性任务。若请求是一次性的查询，那么任务管理器就生成该查询任务并返回运行结果。

循环性任务。请求有一个循环的时间表，任务管理器就将该任务作为持久化数据存储并按照给定的时间表循环执行该任务。

永久性任务。若请求是一个永久性的需要不断执行的任务，任务管理器会定期监视该任务，如果任务瘫痪，任务管理器就重新生成该任务并执行。

2）SOAP 服务器。SOAP 服务器的任务是将功能和任务管理器的接口作为服务的形式，让所有的系统都可以访问到，可以通过一个简单的部署描述文件来完成部署，该文件描述了哪些任务管理器的方法被暴露出来。

3）类服务器。类服务器使得给系统动态加载额外服务成为可能，任务管理器指向类服务器并在类服务器有效时加载所要加载的新的类。这样可以很容易地实现更新、添加和修改任务而不需要重新启动系统。

4）数据库。数据库为任务管理器提供一个持久化的存储场所，数据库存有提交的任务及其相应进度表的详细信息，因此所有提交给系统的任务将会保存下来，即使任务管理器出乎意料地的瘫痪。在每一个循环中，任务管理器查询数据库中的任务并更新相关的记录。

2.3.3 中间件的设计原则

在系统中，对于中间件希望它服务于所有通用的模块以外的各个部分。系统设计出的中间件是一个有弹性的环境，当要加入一个新的标准或者当一个射频识别标准改变了其中的数据格式时，只需修改系统中的相关组件，不必大改整个系统的结构，也不会更改数据库的存储方式，以降低日后系统的维护成本。因此，这里介绍通用的设计方案，以解决目前适应各种不同标准的读写器、标签种类等问题，并希望日后能够改进，提供更好的服务给物流系统中的应用以及相关研究人员。

（1）系统结构设计

从传统的二层结构到现在的多层结构，软件系统的发展经历了很大的变化。传统的应用系统模式是“主机/终端”或“客户机/服务器”，客户机/服务器（Client/Server）系统的结构是指把一个大型的计算机应用系统变为多个能够互为独立的子系统，而服务器便是整个应用系统资源的存储与管理中心，多台客户机则各自处理相应的功能，共同实现完整的应用。

随着中间件与 Web 技术的发展，三层或多层分布式应用体系越来越流行。在这种体系结构中，客户机只存放表示层软件，业务逻辑（包括事务处理、监控、信息排队、Web 服务等）采用专门的中间件服务器，后台是数据库、其他应用系统。系统架构的三层或多层分布式体系结构主要包括如下四个层次：表示层、Web 层、业务层和企业信息系统层。

1)表示层:用于与信息系统的用户进行交互以及显示根据特定规则进行计算后的结果。基于 J2EE 规范的客户端可以是基于 Web 的，也可以是不基于 Web 的独立应用系统。若在基于 Web 的 J2EE 客户端应用中，用户在客户端启动浏览器后，从 Web 服务器中下载 Web 层中的静态 HTML 页面或由 JSP 或 Servlets 动态生成的网页；若在不基于 Web 的 J2EE 客户端应用中，客户端应用程序可以运行在一些基于网络的系统（如手持设备移动产品等）中。同样，这些独立的应用也可以运行在客户端的 Java Applet 中。

2）Web 层：由 JSP 网页、基于 Web 的 Java Applets 以及用于动态生成的网页的 Servlets 构成。这些基本元素在组装过程中通过打包来创建 Web 组件。运行在 Web 层中的 Web 组件依赖 Web 容器来支持诸如响应客户请求和查询 EJB 组件之类的功能。

3）业务层：在基于 J2EE 规范构建的企业信息系统中，将解决或满足特定业务领域商务规则的代码构建成为业务层中的（Enterprise JavaBean）组件。EJB 组件可以完成从客户端应用程序中接收数据、按照商务规则对数据进行处理、将处理结果发送到企业信息系统层进行存储、从存储系统中检索数据以及将数据发送回客户端等功能。部署和运行在业务层中的 EJB 组件依赖于 EJB 容器来管理事务、生命周期、状态转换、多线程以及资源存储等。由业务层和 Web 层构成了多层分布式应用体系结构中的中间层。

4）企业信息系统层

企业信息系统层通常包括企业资源规划（ERP）系统、大型机事务处理系统、关系数据库系统以及其他在构建 J2EE 分布式应用系统时已有的企业信息管理软件。随着 Web 的客户机结构的发展，多层分布式体系的应用将会越来越广泛，中间件作为分布式体系应用中的关键技术，以其独特的优势为各种分布式应用的开发注入了强大动力，极大地推动了应用系统集成的发展。

5）多层应用体系结构特点

在三层结构的逻辑层之间，建立起两级间的映射关系，当其中一层发生改变时，不对系统整体构成影响，这可以降低系统的维护代价。在多层应用体系结构可以平衡各结点的负载情况下，充分利用网络资源，用户使用标准的浏览器（如Ⅲ）通过 Internet 和 HTTP 协议访问服务方提供的 Web 服务器，Web 服务器分析用户浏览器提出的请求等。如果有数据库查询操作的请求（包括修改、添加一记录等），则将这个请求传递给 Web 服务器和数据库之间的中间件。

（2）系统架构

面向服务架构层次划分方法要适合使用和构建服务，也是采用 SOA 架构的重要前提。物联网中间件解决方案的架构就是基于这种 SOA 分层方法的。每一层都有一组明确的功能，而且都利用定义明确的接口与其他层交互。分离组件使应用有了更好的可维护性和可扩展性。下面详细介绍解决方案架构中的每一层。

1）表示层：表示层提供配送中心、供应商门户、零售店门户三类。表示层中所有组件起的都是系统接口的作用。这些接口使用户得以向系统发出请求。并提供了这三类的15 种功能，其中上下文管理功能单位就是沟通用户间的数据编码规则，以便双方有一致的数据形式，能够使用户间互相认识，以用户阅读的方式整合第三方 EIS 和服务。灵活的导航系统方便使用内容管理功能。可定制的外观和感受可以为不同的用户群体提供不同的信息。

2）业务流程：业务流程层囊括了应用对工作流的所有需要。它提供了使业务流程自动化和减少或消除为完成业务流程所需的人工干预的能力。业务流程层协调服务、数据源和人之间的交互，从而实现业务流程自动化。连接 RFID 解决方案最重要的一个接口就是通过业务流程层实现的。由于 RFID 解决方案主要是解决集成问题，事件模型和 RFID 消息总线是该架构的两个关键组件，而且为接入系统的主要接口。RFID 消息总线负责将放置在总线上的消息传送给一个或多个感兴趣的接收者。这一层的构成中还包含一组与 RFID 相关的业务流程，负责处理那些到达消息总线的消息。本层中的业务流程是消息总线上事件的使用者。业务流程层通过意义明确的接口，与服务层和集成层进行通信。

3）服务层：服务层是执行业务逻辑和进行数据处理的地方。它还提供了用于支持企业应用的重要基础架构。服务层最常见的组件是 EnterpriseJavaBeans（EJB，Java 企业柄，Java 核心代码，是 J2EE 的一部分）和面向 Web 服务接口的定制控件。控件是较新的 Java 结构，使用它时开发者不必了解复杂的 J2EE 就可以构建业务逻辑。由开发人员构建业务逻辑，由 BEAWebLogic Workshop 框架创建适当的 J2EE 结构（如无状态会话 bean、有状态会话 bean、实体 bean、消息驱动 bean 等），从而提供希望得到的操作。服务层依赖集成层从不同的外部源获得所需的数据、存储数据和向/从其他相关系统发送/接收信息。

4）集成层：该层提供访问 RFID 应用以外其他企业信息系统的功能，管理系统可通过 WebLogic Portal 来管理服务提供商接口。访问 PIM、ONS 和 EPC-IS 可以通过 Web 服务接口实现。采用适当的方法访问其他系统的方法也有许多，如 JCA 适配器、数据引擎以及 Web 服务等。最终的目标是向标准统一且免费的方向发展。因物联网技术较新，很多实用技术和产品正在发展之中，目前有效的配制方法是利用适配器，它们使利用源数据浏览和进行 XML 转换变得非常轻松。

目前在集成技术方面 Java 是常被采用的技术，它的消息服务（JMS）提供了一种异步方式与外部系统集成的方法，可以实现系统的多种要求。JMS 不仅使系统能够对后端系统进行异步呼叫，同时还可使后端系统也可以在物联网解决方案中发起异步处理。例如，处理传入读写器事件就是由 RFID 解决方案异步完成的。数据集成是 SOA 中又一个可提供服务的领域，用于管理数据的控件可以被展现为提供数据访问功能的服务。

2.3.4　中间件设计目标与功能实现

中间件应用越来越多广泛，已成为解决众多系统问题的基本手段。在三网融合以及与物联网的步融合中，如基于 Java 技术的中间件以及面向 DVB 广播电视接收器、IPTV 终端和 Blu-Ray 播放器等末端设备和头端系统的数字电视中间件标准已经广泛应用，如 GEM 欧洲 ETSI 标准和 ITU 推荐标准，已成为今天的主流。在物联网中的软件和硬件中，应用的软件又被称为中间件。此外物联网领域还由一些“硬”的中间件，如 RFID 在物联网中，它也可称为一种“硬”的中间件。根据不同的特点和技术阶段，还可进行不同的定义。如在安防领域，随着应用功能的增加和复杂度的提高，形成了“大安防”的理念，系统涉及各种终端形态、智能识别、GIS、门禁、报警监测、停车场管理、SCADA、流媒体交换、视讯会议、应急管理与联动、安检防范、消防联网、国土资源安全（地震灾害、滑坡、桥梁、隧道监测等）、电工考场、教学应用等各种业务。安防应用集成中间件的概念应运而生，国内一些安防专家已开始研发安防中间件。

（1）设计目标

在物联网中间件的设计中，读写器在读取 RFID 标签并识别出数据编码后，可对读取进来的标签信息进行数据平滑、校验以及暂存等一些列操作。数据经过中间件进行处理，对于不同标准的读写器，要考虑系统的维护成本。如能加入一个新的标准或者当一个 RFID 标准改变了其中的数据格式，只需修改系统的相关组件，而不必改动整个系统的结构，这样就不会变更数据库的存储方式，就可降低系统的成本。

（2）功能实现

中间件不仅可以为应用程序提供集成功能，还可以提供数据过滤功能来减少从读写器到应用程序的数据量，同时为标签物体或其他对象提供与应用程序之间的稳定通信和实时信息。通常物联网中间件具有读写器接口、事件管理器、应用程序接口、目标信息服务（Object Information Service，OIS）以及对象名解析服务（ONS）等功能。物联网中间件的功能模块结构如图 2-11 所示。

1）读写器接口。

物联网中间件必须优先为各种形式的读写器提供集成功能，读写器接口即是实现此项功能的重要组成部分。协议处理器确保中间件能够通过各种网络通信方案连接到 RFID 读写器，如 RS-232、TCP/IP 等接口及各自的数据交换协议与应用程序通信，因此协议处理器使得来自很多不同生产厂商的读写器能够以无缝方式与中间件应用程序相互作用。早期的读写器只用唯一的通道周期性地轮流检测读写器来得到标签数据，但如今开发出的读写器有两个通道：一个是所谓的控制通道，用来处理应用程序发出的指令和对应用程序的响应；另一个是通知通道，它取代了轮流检测方式以异步方式自动将标签信息传输给应用程序。

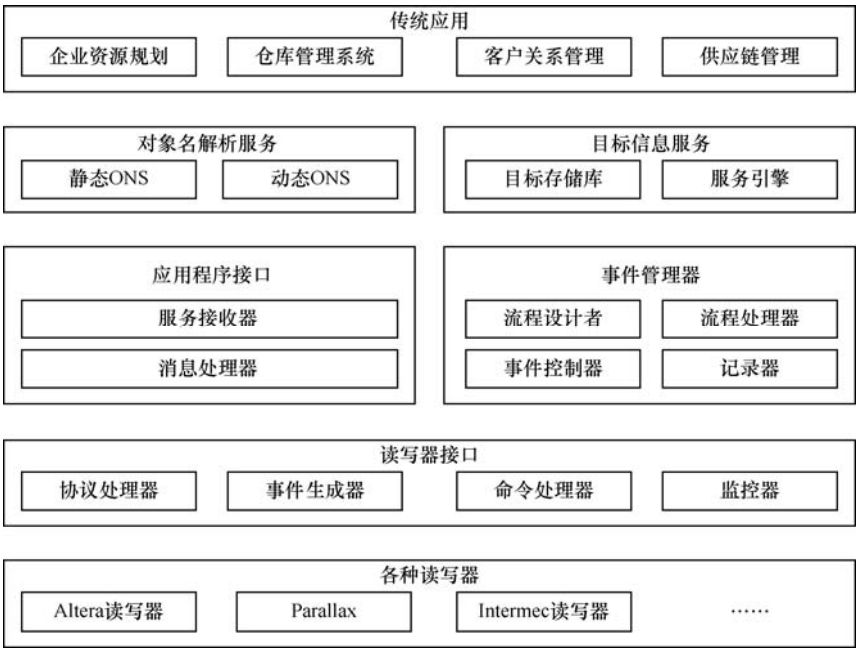


图 2-11　物联网中间件功能模块结构

读写器完成阅读后，读得的标签数据以该阅读周期被发送到应用程序。只要标签在读写器的工作范围内，对它的阅读指令就被不断地发送给应用程序。同时，所制定的规范提出了根据减少引入的标签数据规模的需要确定事件产生的办法。每当标签被第一次发现时，便产生事件“TagSeen”。当标签在某时间段内瞄准一系列阅读周期时，便产生“FirmRead”事件。若标签先前产生了一个“Finn Read”事件，但是还没有到预先已设定的时间间隔，则产生一个“Tag Expired”事件；此外，若标签的状态保持在“SoftRead”状态而且标签不被阅读，则此时会发出“TagVanished”事件。这种方法去除了对于相同标签的多余传送步骤，使进入的信息量大为减少。

事件生成器在物联网中间件中发挥着重要作用，不但为每个引入的标签数据生成事件并传送给事件管理器，而且类似模拟器那样为了支持应用程序的开发，在没有物理读写器连接时产生虚拟标签事件数据。

2）事件管理器。

事件管理器（EM）用于对来自读写器接口的 RFID 事件数据进行过滤、聚合和排序操作，并且再通知数据与外部系统相关联的内容。从读写器会接收大量的数据，进行适当的过滤处理就显得尤其重要，除去那些多余的和非必需的信息。过滤所使用的规则主要取决于所涉及的服务类型。

过滤器用来去除多余的标签阅读事件，提高阅读区域和物体运动的速率。在完成阅读任务读写器，系统会将冗余数据包告给应用程序，直到标签离开该区域为止。由于 RFID 读写器不能百分之百准确地报告标签数据，或当此区域附近有未预料到的标签物体经过时也可能产生意外读取，此时则需要应用滤波算法。这就类似于读写器接口的数据生成器的“FinnRead”事件的功能，每个标签都有其唯一的 ID，若该 ID 和预先设定的编码相匹配，则过滤器允许其传输到应用程序，当两者不匹配时就会被忽略掉。若标签物体被放在一起，则多个读写器能够报告相同的标签数据，而且结果与相同的语法操作有关。例如，当读写捕捉某仓库的进货数据情况时，就需要应用协调算法从来自众多的读写器标签数据中选择一个数据。是否过滤标签数据，要看有关事件是否与用户应用程序相关联。过滤的数据能够被快速传给其他过滤器进行更深入的处理，或者为了发送到外部程序而先记录下来。

3）应用程序。

接口应用程序是使应用程序能够控制读写器，其中服务接收器（SL）接收应用程序系统的指令，提供 XML-RPC、SOAP-RPC、Web-Service 类的通信功能。消息处理器分析传送的指令，并将其结果传送到读写器接口中的命令处理器，命令处理器响应后传回应用程序系统。

Auto-ID 中心通过 Savant 设计应用程序接口，包括三个区分明显的层，如图 2-12 所示。内容层对在 Savant 和应用程序之间进行交换的抽象信息进行详细解释。信息层详细说明抽象的信息是怎样被编码、封装和转换的。传输层有两种信息通道。其一是控制通道，用于 Savant 和应用程序之间的请求/响应命令；其二是通知通道，用于由 Savant 将单向传输的信息异步地传送给应用程序。几乎所有的读写器都不同时支持两种信息通道。因此，要求中间件必须提供相应模块，通过执行控制通道的轮流检测机制实现两种信息通道。

4）对象信息服务。

对象信息服务（OIS）由两部分组成：一个是目标存储库，用于存储与标签物体有关的信息并使之能供后续查询；另一个是服务引擎提供目标存储库管理的信息接口。

（3）结构选择

系统结构的选择是十分重要的，计算机体系结构经历了从主机集中的终端方式、C/S 结构、B/S 结构，以及现在使用越来越普遍的多层次客户端服务器结构。传统的分布式系统采用客户端/服务器两层结构，客户端往往过于庞大，负载过重，导致“胖客户端”产生，而且系统维护成本提高。在这种传统模式下开发的系统，移植性和可扩展性较差，开发和维护繁杂，不能适应不断增长的多方面需求。分布式多层结构模式的出现很好地解决了两层 C/S 结构的上述问题。三层结构描述是将客户端的事务处理逻辑独立出来而单独构成一层，即应用层。这样，客户层、应用层和原有的数据层便形成了一个三层体系结构，如图 2-13 所示。

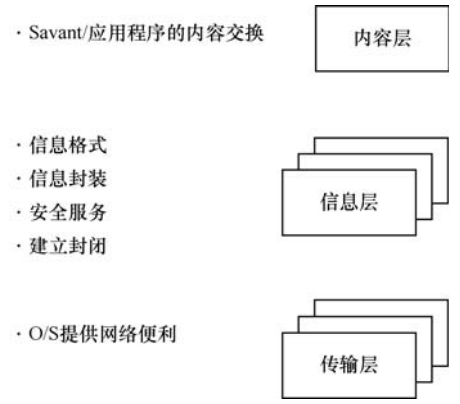


图 2-12　应用程序接口的层次结构

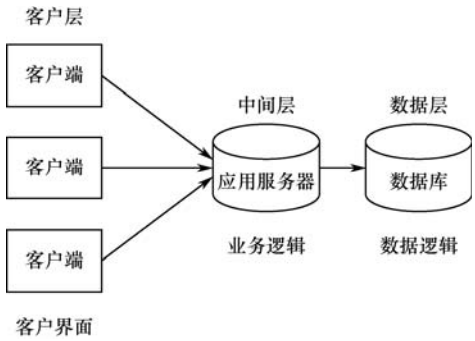


图 2-13　中间件三层体系结构

在以中间件为平台的应用系统中，客户端提出的服务请求不是直接提交给数据库，而是通过中间件提供的高速数据特点传送至服务器端，进而提交数据库。同时交易服务中与数据库无关的逻辑处理也由中间件完成，这样就分担了很多原来需要数据库完成的工作，提高了系统的工作效率。

客户层又称为表示逻辑层，其表现形式为用户界面，其主要功能是实现用户交互和数据表示，为以后处理收集信息，向第二层业务逻辑请求调用核心服务处理，并显示结果。

应用层又称为业务逻辑层，实现核心业务逻辑服务，将这些服务按名字广播、管理并接受客户服务请求，向资源管理器提交数据操作，同时将处理结果返回给请求者、客户或其他服务器。

数据层又称为数据逻辑层，负责管理应用系统数据资源，完成数据操作；中间层的服务器组件在完成服务的过程中，通过本层资源管理存取相关数据。

中间件三层结构模式是应用系统的基础，既作为底层支撑环境，又作为客户端和服务器的连接纽带，使系统成为一个有机、高效的整体，它主要提供下面两个功能：

1）负责客户端与服务器之间的联系与通信，并提供了表示层和业务层之间、业务层与业务层之间、业务层与数据层之间、数据层与数据层之间的连接和完善的通信机制。

2）提供了一个三层结构应用开发和运行的平台。

中间件为建立运行、管理和维护三层的体系结构的应用提供了一个基础框架，降低了应用开发、管理和维护的人力、物力成本，提供了成功率，真正使大型企业应用的高效实现成为可能。

2.3.5　设计平台

物联网中间件的实现需要一定的平台，本节主要介绍实现中间件的技术标准，主要有 COM、CORBA 及 J2EE 等。

（1）组件对象模型 COM

最初作为 Microsoft 桌面系统的构件技术，主要为本地的 OLE（Object Linking and Embedding，对象连接与嵌入）应用服务，但是随着 Microsoft 服务器操作系统 NT 和 DCOM（Distributed COM，分布式组件对象模型）的发布，COM 通过底层的远程支持使得构件技术延伸到了分布式应用领域。COM 是 Microsoft 提出的一种组件规范，其多个组件对象可以连接起来形成应用程序，并且在运行时，可在不重新连接或编译的情况下被卸下或换掉。COM 既是规范，也是实现方式，它以 COM 库（OLE32.d11 和 OLEAut.d11）的形式提供了访问 COM 对象核心功能的标准接口及一组 API 函数，这些 API 用于实现创建和管理 COM 对象的功能。COM 把组件的概念融入到 Windows 中，但其只能使本机内的组件进行交互，DCOM 则为分布在网络上不同结点上的组件提供了交互能力。MTS（Microsoft Transaction Server）针对企业 Web 的特点，在 COM/DCOM 的基础上添加事务特性、安全模型等服务。COM+把 COM 组件的应用提升到应用层，它通过操作系统使组件对象模型建立在应用层上，把所有组件的底层细节（如目录服务、事务处理、连接池及负载平衡等）留给操作系统。尽管有些厂商正在为 UNIX 平台使用 COM+而奋斗，但 COM+基本上仍是 Windows 平台的解决方案。

（2）通用请求代理体系结构

分布式计算技术是 OMG 组织基于众多开放系统平台厂商提交的分布对象互操作内容的公共对象请求代理体系规范。CORBA 分布计算技术是由绝大多数计算平台厂商所支持和遵循的系统规范技术，其模型完整、先进，独立于系统平台和开发语言，得到广泛的支持，已逐渐成为分布式计算技术的标准。COBRA 标准主要分为对象请求代理、公共对象服务和公共设施三个层次。最底层是对象请求代理（ORB），规定了分布式对象的定义（接口）和语言映射，实现对象间的通信和互操作，是分布式对象系统中的“软总线”。在 ORB 之上定义了很多公共服务，如并发服务、名字服务、事务服务、安全服务等。最上层的公共设施则定义了组件框架，提供可直接为业务对象使用的服务，规定业务对象有效协作所

需的协定规则。CORBA 是编写分布式对象的一个统一标准，这个标准与平台、语言和销售商无关。CORBA 包含了很多技术，而且范围十分广泛。其中 IIOP（InternetInterORBP-rotoc01）协议是 CORBA 的标准因特网协议，运行在分布式对象通信的后台。CORBA 中的客户通过 ORB 进行网络通信，使通信变得非常容易。CORBA 中的接口语言（IDL）用于定义客户端和它们调用的对象之间的接口，是与语言无关的接口，定义后可以用任何面向对象的编程语言来实现。

（3）企业版 J2EE 标准

为了推动基于 Java 的服务器端应用开发，J2EE 是当前异构数据集成普遍采用的标准。Java、XML 等中间件关键技术都是 J2EE 技术体系的一部分。J2EE 是提供平台无关的、可移植的、支持并开发访问和安全的，完全基于 Java 的开发服务器端中间件的标准。在 J2EE 中，Sun 给出了完整的基于 Java 语言开发面向企业分布应用的规范。其中，在分布式互操作协议上，J2EE 同时支持 RMI 和 IIOP；而在服务器端分布式应用的构造形式，则包括了 Java Servlet、JSP（Java Server Page）、EJB 等多种形式，支持不同的业务需求，Java 应用程序具有“Wrke once，mn anywhere”的特性，使得 J2EE 技术在分布式计算领域得到了快速发展。

J2EE 和 CORBA 的最大区别是，CORBA 只是针对单个对象，而不是被应用服务器自动管理的可部署的服务器端组件。CORBA 的特点是大而全，互操作性和开放性非常好；缺点是庞大而复杂，并且技术和标准的更新相对较慢，COBRA 规范从 1.0 升级到 2.0 所花的时间非常短，但后续版本的更新发布就十分缓慢了。

（4）相关性分析

针对上述三个技术标准，通常从集成性、可用性和可扩展性三个方面对分布式计算平台进行评价分析，主要内容和要素见表 2-4。

表 2-4　三种主流分布式计算平台

性 能 平 台		COM	CORBA	J2EE
集成性	跨语言性能	好	好	好（限于 Java）
	跨平台特性	差（限于 Windows）	好	好
	网络通信	一般	好	好
	公共服务构件	一般	好	一般
可用性	事务处理	一般	好	一般
	信息服务	一般	一般	一般
	安全服务	一般	好	好
	目录服务	一般	好	一般
	容错性	一般	一般	一般
	软件开发商支持度	好	一般	好
	产品成熟性	好	一般	一般
可扩展性		一般	好	好

1）集成性：集成性主要反映在基础平台对应用程序互操作能力的支持上，它要求分布在不同机器平台和操作系统上，采用不同的语言或者开发工具生成的各类商业语言必须能集成在一起，构成一个统一的企业计算框架。这一集成框架必须建立在网络的基础之上，并且具备对语言的集成能力。

2）可用性：要求采用的软件构件技术必须是成熟的技术，相应的产品也必须是成熟的产品，在企业应用中能够稳定、安全、可靠地运行。

3）可扩展性：集成框架必须是可扩展的，能够协调不同的设计模式和实现策略，可以根据企业的需求进行裁剪，并能迅速反映市场的变化和技术发展趋势。通过保证当前应用的可重用性，最大程度地保护企业投资。

2.4　无线测距定位技术

定位技术在物联网中可用于目标跟踪，实时监视目标的行动，以及预测目标的轨迹路径。根据结点的地理位置信息来构建网络拓扑，实时统计网络覆盖情况，在结点密度低的地区，及时采取必要措施，改进网络管理。只有获得了对象或结点的位置信息，传感器收集的信息才有实际意义。在环境监测过程中，可以及时确定火灾位置，确定战场上敌人的车辆的地点和区域，在管道泄漏时实现定位，可以给决策和采取措施提供基本依据。因此，无线结点定位技术是传感器网络的基本功能之一。基于测距技术的无线传感器网络定位算法比非测距技术的传感器网络定位算法精度高，所以本节的重点是介绍基于测距技术的无线传感器网络定位技术。

无线传感器网络中，结点通过飞机散布、人工排列方式，大量部署在被感知物体内或附近，这些结点通过自组织方式构成无线网络，以协作的方式感知、采集和处理网络覆盖区域中的特定信息，可以实现在任意位置和任何时间的信息采集、分析和处理。在传感器网络结点定位技术中，根据结点是否已知自身的位置，把传感器结点分为信标结点或锚结点（beacon node or anchor node）和未知结点（unknown node）。信标结点在网络结点中的比例小，可以应用定位装置或手动部署手段来获取它们自身的精确位置。信标结点是未知结点的定位参考点。除了信标结点外，其他传感器结点都是未知结点，它们通过信标结点的位置信息来确定它们的位置。

根据在定位的过程中，是否需要实际测量结点间的距离，定位算法可以分为：Range-Based 和 Range-free 定位算法。Range-Based 定位测量结点间点对点的距离或角度信息，使用三边测量（trilateration）、三角测量（triangulation）或最大似然估计（multilateration）定位法计算结点位置；Range-free 定位则不需基于距离和角度信息，根据网络连通性等信息

就可以实现定位的目的，DV-Hop 和 MDS-MAP 等都是典型的 Range-free 定位算法，其中 MDS-MA 可以在 Range-Based 的协助下实现更准确的定位。Range-Based 定位常用的测距技术有 RSSI、TOA、TDOA 和 AOA。Range-Based 定位机制还通过使用各种算法来减小测距误差对定位的影响，包括多次测量、循环定位求精等。

2.4.1 结点间测距的基本方法

（1）基于接收信号强度指示（RSSI）

RSSI（Rceived Signal Strength Indicator）通常用于无线射频信号的定位。其工作原理是发射结点发送信号的强度和接收结点接收信号的强度进行比较，再考虑信号在传播过程中的损失，使用理论或信号传播模型将传播损耗转化成距离。显然，该损耗值随距离的增加而增加，未知结点可以通过计算 RSSI 值来确定其与发射信号的锚结点之间的距离。传感器结点通常具有通信能力，因此通过通信控制芯片可以直接测量距离，而没有额外的硬件资源损耗。在无线传感器网络中，理论上通过三个锚结点应用 RSSI 定位方法就可以三边测量方法确定未知结点的位置信息。在实际应用环境中，由于复杂环境中的多径干扰，非视线关系等因素，该方法的精度不高。但由于所需的硬件设备少，与现实设备中的许多无线通信模块都可以直接提供 RSSI 值，因此 RSSI 定位方法被广泛使用。无线电传播路径损耗对于基于接收信号强度指示定位算法最后的精度有很大的影响，在实际应用中，由于考虑了多径、扰射、障碍等因素，使模型非常复杂，需要考虑的因素很多，目前普遍使用的是自由空间无线电传播路径损耗模型，其公式为

$$\mathrm{Loss} = 32.4 + 10\lg(d) + 10k\lg(f) \tag{2-1}$$

式中，d 为距信源的距离，单位一般为 km；f 为频率，单位为 MHz；k 为路径衰减因子，其值一般为 2～4。因为在许多实际的应用环境中，需要考虑的因素更为复杂，无线电传播路径损耗与真实值可能有一定的偏差，式（2-2）中的对数常态模型则更加合理，这个公式可以用来计算锚结点接收到消息时的路径损耗，即

$$\mathrm{LS}(d) = \mathrm{LS}(d_0) + 10k\lg\frac{d}{d_0} + X_\sigma \tag{2-2}$$

式中，$\mathrm{LS}(d)$ 表示经过了距离 d 后的路径损耗；X_σ 为平均值为零的高斯分布随变数，其取值范围一般为 4～10；取 $d=1$ 代入式（2-1）便可求得 Loss 值，即为式（2-2）中的 $\mathrm{LS}(d_0)$，继而可以求出路径损耗 $\mathrm{LS}(d)$。所以，各个结点收到的信号强度为

$$\mathrm{RSSI} = P + G - \mathrm{LS}(d) \tag{2-3}$$

式中，P 表示结点发射功率，G 表示天线增益。

（2）基于到达时间（TOA）

基于到达时间的工作原理是通过测量信号在两个结点之间的传输时间来实现定位，当传

输信号的传播速度是已知的，然后根据信号的结点之间的传播时间来计算它们之间的距离。传输时间是指无线信号从锚结点发送信号到未知结点接收信号的时间。用此方法进行定位的过程中，非常重要的一点是，结点之间有非常精确的时间同步。因此，锚结点到未知结点发送一个信号时，都会在发送的数据包内标识时间戳，未知结点接收到数据包后就可以计算接收这个信号所使用的时间。TOA 测距的精确性相对于 RSSI 更高，但前提是需要非常精确的时间同步，这对传感器结点硬件提出了更高的要求。在短距离测量中这个问题更为突出。

TOA 距离测量误差有两个主要方面：一方面，主要误差来源是复杂环境中的多径和非视距传播等客观因素所造成的时间延迟；另一方面，则来源于结点本身的距离测量设备，如时间同步没有达到绝对精度。这种误差将会随着定时技术的发展而逐渐减少。

（3）基于到达时间差（TDOA）

TDOA 时差测距技术的工作原理是，在发送结点的同时发送不同传播速度的信号（通常使用无线射频或超声信号），未知结点记录两种信号到达时间差，并通过它们的传播速度，来计算结点间距离。这种技术的优点是不需要严格的时钟同步，从而实现起来比 TOA 更简单，定位精度更高。像现在熟悉的 Cricket、AHLos（Ad Hoc Localization System）定位系统都是利用时差测量结点间的距离。但这种方法仍存在一些问题，比如超声波传播距离有限，NLOS 对超声波信号的传播影响过大等。同时，它需要传感器结点在同一时间能同时感知两种不同信号的能力，所以在硬件的设计上更为复杂。

（4）基于到达角度（AOA）

AOA 的定位方法是，通过阵列天线或多个接收机得到不同方向的相邻结点发送的信号，接收结点通过天线阵列或多个超声波接收器感知发射器发送的信号到达的方向，计算接收结点和发射器之间的相对位置和角度，从而构成从接收器到发射器的方位线。两方位线的交点是未知结点位置。AOA 测距技术容易受到外部环境的影响，并且需要复杂的硬件设备，在硬件规模和功耗上不适用于大规模传感器网络。在一个特定的应用中，假设有 N 个发送结点参与定位，坐标值为 (x_i, y_i) 各发射结点到待定位结点的波的方向 θ_i，则待定位结点坐标（x，y）可表示为

$$\theta_i = \arctan[(y_i - y)](x_i - x)\varepsilon_i, \qquad i=1，2，3，\cdots，N \tag{2-4}$$

式中，ε_i 表示估计误差，服从零均值的高斯分布。上面方程可以转化为

$$\tan(\theta_i)x - y = \tan(\theta_i)x_i - y_i + \varepsilon_i, \qquad i=1，2，3，\cdots，N \tag{2-5}$$

通过上式即可求出未知结点位置。

2.4.2　计算结点位置的基本方法

无线传感器网络定位的过程中，如果已知锚结点和未知结点的距离或相对的角度，可使用下面的方法计算未知结点位置。

（1）三边测量法

在基于距离的定位算法中，三边测量法是计算未知结点坐标经常用到的方法。如图 2-14 所示，已知三个锚结点 A_1、A_2、A_3 的坐标分别为 (x_1,y_1)，(x_2,y_2)，(x_3,y_3)，它们到待定位结点 B 的距离分别为 d_1，d_2，d_3。假设 B 点的坐标为（x，y），则可通过以下公式计算出 B 点坐标值：

$$(x-x_i)^2+(y-y_i)^2=d_i^2，\ i=1，2，3 \qquad (2\text{-}6)$$

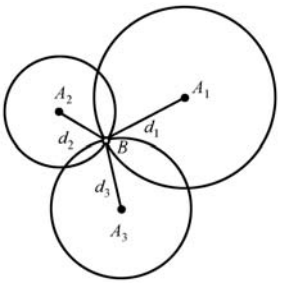


图 2-14　三边测量示意图

一般情况下，可以求解出：

$$\begin{bmatrix}x\\y\end{bmatrix}=2\begin{bmatrix}x_1-x_3 & y_1-y_3\\ x_2-x_3 & y_2-y_3\end{bmatrix}\begin{bmatrix}x_1^2-x_3^2+y_1^2-y_3^2+d_1^2-d_3^2\\ x_2^2-x_3^2+y_2^2-y_3^2+d_2^2-d_3^2\end{bmatrix} \qquad (2\text{-}7)$$

（2）三角测量法

三角测量法是针对 AOA 测距来求结点间坐标的，原理如图 2-15 所示，三个锚结点 A、B、C 坐标分别为 (x_a,x_a)，(x_b,x_b)，(x_c,x_c)，待定位结点 D 相对于结点 A、B、C 的角度分别为：$\angle ADB$，$\angle ADC$，$\angle BDC$。假设结点 D 的坐标为（x，y）。对于结点 A、C 和角 $\angle ADC$，如果弧段 AC 在 $\triangle ABC$ 内，则能够唯一确定一个圆，设圆心坐标为 $O_1(X_{01},Y_{01})$，半径为 r_1，则有 α 角为 $\angle AO_1C=(2\pi-\angle ADC)$，且有下列公式成立：

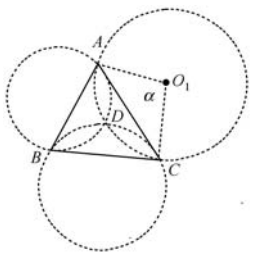


图 2-15　三角测量法示意图

$$\begin{cases}\sqrt{(x_{01}-x_a)^2+(y_{01}-y_a)^2}=r\\ \sqrt{(x_{01}-x_c)^2+(y_{01}-y_c)^2}=r_1\\ (x_a-x_c)^2(y_a-y_c)^2=2r_1^2-2r_1^2\cos\alpha\end{cases} \qquad (2\text{-}8)$$

由式（2-8）可求出 O_1 坐标值和 r_1。同理可求出另外两边及夹角所对应的圆心坐标和半径值，最后利用三边测量法得出 D 点坐标。

（3）最大似然估计

最大似然估计的计算原理大体上与三边测量法类似，其基本思想是假如一个结点可以获得足够多的信息来形成一个由多个方程式组成并拥有唯一解的超限制条件或限制条件完整的系统，那么就可以同时定位跨越多跳的一组结点，如图 2-16 假设 n 个锚结点的坐标分别为 (x_1,y_1)，(x_2,y_2)，(x_3,y_3)，…，(x_n,y_n)，它们到待定位结点 P 的距离分别为 d_1，d_2，d_3，…，d_n，设 P 的坐标为（x，y），则

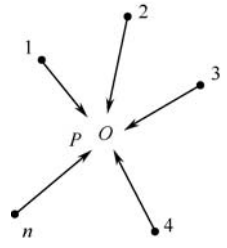


图 2-16　最大似然估计法示意图

$$(x-x_i)^2+(y-y_i)^2=d_i^2，\ i=1，2，3，\cdots，n \qquad (2\text{-}9)$$

由标准的最小二乘法可以算出待定位结点 P 的坐标：

$$\hat{\boldsymbol{X}} = (\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}b \tag{2-10}$$

其中，

$$\boldsymbol{A} = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix} \qquad b = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 + d_n^2 - d_1^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_n^2 - d_{n-1}^2 \end{bmatrix}$$

（4）基于泰勒展开的最小二乘法（Tarlor-LS）

利用最大似然估计求式（2-9）时，势必会通过方程相减的方法来消去方程中的二次项，这样以来单纯的坐标相减可能对已知的坐标信息会有损失，为了充分利用已知结点的坐标信息，采用泰勒展开对二次方程进行线性化处理。

令
$$f(x,y) = (x - x_i)^2 + (y - y_i)^2 \tag{2-11}$$

对上式在点 (x_0, y_0) 进行泰勒展开有

$$\begin{aligned} f(x,y) = f(x_0 + h, y_0 + k) = & \sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2} \\ & + \frac{(x_0 - x_i)}{\sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2}} h \\ & + \frac{y_0 - y_i}{\sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2}} k \end{aligned} \tag{2-12}$$

将式（2-12）代入式（2-9）有

$$\begin{cases} \dfrac{(x_0 - x_1)}{\sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2}} h + \dfrac{(y_0 - y_1)}{\sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2}} k = d_1 - \sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2} \\ \dfrac{(x_0 - x_2)}{\sqrt{(x_0 - x_2)^2 + (y_0 - y_2)^2}} h + \dfrac{(y_0 - y_2)}{\sqrt{(x_0 - x_2)^2 + (y_0 - y_2)^2}} k = d_2 - \sqrt{(x_0 - x_2)^2 + (y_0 - y_2)^2} \\ \vdots \\ \dfrac{(x_0 - x_n)}{\sqrt{(x_0 - x_n)^2 + (y_0 - y_n)^2}} h + \dfrac{(y_0 - y_n)}{\sqrt{(x_0 - x_n)^2 + (y_0 - y_n)^2}} k = d_n - \sqrt{(x_0 - x_n)^2 + (y_0 - y_n)^2} \end{cases} \tag{2-13}$$

(x_0, y_0) 的初始值取为锚结点的中点，采用最小二乘法解方程。解得的 h、k 的值来判断式（2-14）是否成立。

$$\sqrt{h^2 + k^2} < \varepsilon_{\text{threhole}} \tag{2-14}$$

若上式成立，则停止计算；否则，将 (x_0, y_0) 增加步长（h/2，k/2）后代入式（2-13）重新计算，直到条件式（2-14）成立，此时求得的 (x_0, y_0) 即为所求结点的坐标。当约束条件过少时，最小二乘法中的循环求解过程有可能出现奇异值的问题，此时用次梯度坐标计算

方法进行求精。建立函数 $s(X)$ 。

$$s(X)=\frac{1}{2}\sum_{J}(|x_i-x_j|-d_{ij})^2 \tag{2-15}$$

在 $x_i^k-\gamma\frac{\partial S}{\partial x_i}\rightarrow x_i^{k+1}$ 的过程中，坐标的值也在逐渐精确。其中，

$$\frac{\partial S}{\partial x_i}=\sum_{J}(|x_i-x_j|-d_{ij})\frac{(x_i-x_j)}{|x_i-x_j|}$$

2.4.3 定位算法的分类

定位算法的分类有很多种，现介绍几种常见的分类方式。

（1）基于测距（Range-based）的定位和非基于测距（Range-free）的定位

根据在定位的过程中是否需要测量实际的结点间的距离，定位算法可以分为基于测距的（Range-based）定位算法和非基于测距的（Range-free）定位算法。前者需要测量相邻结点间的绝对距离或位置，并利用结点间的实际距离计算出未知结点的位置；后者则无须测量结点间的绝对距离或位置，而是利用结点间的估计距离来计算未知结点的位置。

Range-based 定位算法常用的测距技术包括 RSSI、TOA、TDOA 以及 AOA。RSSI（Received Signal Strength Indicator）虽然具有低功耗、低成本的要求，但可能产生的测距误差达到±50%，误差比较大；TOA（Time of Arrival）需要结点具有精确的时间同步，因此不能用于松散耦合定位系统；TDOA（Time Difference on Arrival）定位技术则由于受到超声波传输距离有限和 NLOS 问题对超声波信号传播的影响，在实用性上受到影响；AOA（Angle of Arrival）则不仅容易受到外部环境的影响，而且需要额外的硬件设备，其硬件规模和功耗都不可用于实际的传感器结点。除了上述定位技术的局限性，Range-based 定位技术采用多种算法降低测距误差对定位的影响，包括重复测量，循环定位求精，这些都会产生大量的计算和通信开销。所以对于 Range-based 来说，定位精度较高是其可取之处，但并不适用于很多低功耗、低成本的应用。

因功耗和成本因素，以及定位精度对大多数应用已足够，Range-free 定位方案备受关注。质心、DV-Hop、Amorphous、APIT 和 MDS-MAP 是现有的 Range-free 定位算法，其中 MDS-MAP 也可在 Range-based 条件下实现更精确的定位。

（2）绝对定位与相对定位

绝对定位和物理定位有着类似的定位结果，都是一个标准的坐标位置，如纬度和经度。相对定位则通常是利用网络中的部分结点作为参考点（锚结点），从而建立整个网络的相对坐标系统。绝对定位为网络提供了一个唯一的命名空间，受结点的移动性的影响较小，具有更广泛的应用空间。但研究发现，在相对定位的基础上可以部分实现路由协议，特别是

基于地理位置的路由（geo-routing），而相对定位则无须锚结点。大多数定位系统和算法都可以实现绝对定位服务，典型的相对定位系统和算法有 SPA（self-positioning algorithm）、LPS（local positioning system）等，而 MDS-MAP 定位算法可以在不同网络配置的基础上实现两种不同的定位。

（3）紧密耦合（tightly coupled）与松散耦合（loosely coupled）

紧密耦合定位系统是指锚结点被精心部署在一个固定的位置，并通过电缆等有线介质连接到中央控制器；松散型定位系统使用的锚结点则采用没有中央控制器的无线分布式协调方式。紧密耦合定位系统的共同特点是适用于室内环境，并具有较高的精度和实时性，时间同步和锚结点间的协调问题容易解决。但紧密耦合定位系统的部署策略限制了系统的可扩展性，代价大，无法应用于无法布线的户外环境。松散耦合系统则没有紧密耦合系统的精确性，但获得了部署的灵活性，依靠锚结点和未知结点的协调和信息交换来实现定位。在松散耦合系统中，因为网络的部署依靠 ad-hoc 方式，锚结点之间没有直接的协调，所以会出现信道竞争和相互干扰的情况。

这种分类方法与基于基础设施和无需基础设施（infrastructure-based versus infrastructure-free）的分类方法相似，不同的是后者以整个系统除了传感器结点外是否还需要其他设施为标准。

（4）集中式（centralized computation）计算与分布式（distributed computation）计算

集中式计算的基本思想是将每个结点所需的信息传送到一个中央结点，然后通过中央结点计算出每个未知结点的位置信息，该算法不受计算和存储性能限制的影响，定位精度较高，但由于定位过程中的计算操作都由一个中央结点来完成，因此中央结点可能会由于过多的通信开销而过早地消耗全部能量，从而造成网络信息交流受阻或中断，缩短了整个网络的生命周期。集中式计算算法包括凸规划算法、MDS-MAP 算法等。分布式计算算法是依赖于结点间的信息交换和协调，通信量比较小，能量消耗较低，计算简单，算法具有良好的可扩展性。与集中式算法相比，它具有更大的灵活性。质心算法、Dv-Hop 算法和 APIT 算法等都属于分布式算法。

（5）递增式定位算法和并发式定位算法

这种分类法是根据计算结点位置的先后顺序来区分的，递增式算法一般是由几个结点的定位开始，其他结点根据其与已完成定位的结点之间的距离或角度信息，采用极大似然法或局部最优策略逐步完成对位置的估计。利用递增式算法，最大的缺点是在定位过程中有较大的误差累积。并行算法的结点定位以并行的方式同时进行位置的计算。许多迭代优化算法就属于并行算法，该算法可以较好地避免局部最小值和误差累积。因此，在实际应用中这种算法的应用也更广泛。

2.4.4 定位算法的性能评价

无线传感器网络的定位算法是与应用息息相关的，所以定位性能的好坏直接影响其实际使用情况，如何评价定位算法和系统的好坏是一个值得深入研究的问题。下面论述几种常用的定位系统和算法的评价标准。

1）定位精度。毫无疑问，定位精度是定位技术的重要评价指标，因为在实际应用中，定位系统只有在满足一定的定位精度的前提下才有使用价值。其数值一般用误差值和结点无线射程的比表示，如定位精度 18%就表示定位误差相当于结点的无线射程的 18%。还有一部分定位系统将二维网络部署区域划分为很多网格，其定位精度也就等于网格的大小。

2）锚结点密度。绝大部分的网络，锚结点密度高，定位精度也更高。而锚结点位置一般依靠人工部署和全球定位系统来获得。当使用人工部署锚结点时，不仅受到网络部署环境的限制，同时也限制了网络和定位算法的可扩展性；当使用全球定位系统对锚结点进行定位时，锚结点的成本比普通结点高两个数量级以上，换句话说，假设一个网络中有 10%个结点是锚结点，整个网络的成本将增加 10 倍。因此，定位系统的锚结点密度是算法性能评价的重要指标之一。

3）结点密度。结点密度对无线传感器网络的连通性有直接影响。在网络中，结点密度越高，网络连通性越强，就可以获得更多的定位辅助信息，但这也意味着需要更多的网络部署成本，因为结点间的通信会使有限的带宽更加拥挤。与此相反，结点稀疏的无线传感器网络的定位性能将下降。

4）定位规模。不同的定位系统和算法，其有效的定位规模也是不一样的。并且，在一定时期内，不同的定位系统，其能够定位的结点数目也是不同的。此外，给予一定数目的基础设施或在一段时间，这种技术可以定位多少目标也是评价定位系统和算法的一个重要的评价指标。

5）容错和适应。通常，定位系统和算法都需要好的无线通信环境和可靠的网络结点设备。但在实际应用环境中，多径传播、衰减、非视距（Non-Line-Of-Sight，NLOS）等问题都会影响定位精度；网络中的结点会由于周围环境或人为原因等（如电池耗尽，自身损伤）出现故障。在一些特殊环境中，想通过物理修复或更换传感器结点，或使用其他高精度的测量手段往往会很困难或根本不可能。因此，定位系统和算法的软、硬件必须具有很强的容错性和适应性，可以自动调整或纠正错误，适应特殊环境，减少各种影响带来的误差，提高定位精度。

6）消耗功率。由于传感器结点本身的特点，以及电池能量的有限，在实际应用环境中想要更换电池在很多时候是不可能的。在保证定位精度的前提下，实现定位和功耗是密切相关的，其中包括通信成本、存储成本等。

在实际应用中，究竟是用某一个指标或几个指标的组合，应根据具体的使用要求和硬件和软件设置。

2.5 其他无线测距定位技术

随着数据业务和多媒体业务的迅速增加，定位和导航的需求增加了，特别是在复杂的室内环境，如机场大厅、展厅、仓库、超市、图书馆、地下停车场以及矿井环境，往往需要确定移动终端或其持有人、设施和物品在室内的位置信息。但目前，在室内环境和条件下定位技术精度不高，完善的定位技术不能很好地得到应用。因此，专家和学者们提出了许多的室内定位技术的解决方案，如 A-GPS 定位技术、超声波定位技术、蓝牙技术、红外技术、射频识别技术、超宽带技术、无线局域网、光学跟踪和定位技术、图像分析和计算机视觉定位技术等。这些室内定位技术一般可分为几类，如 GNSS 技术（如伪卫星）、无线定位技术（无线通信信号、无线射频标签、超声波、光学跟踪、无线传感器定位技术、计算机视觉、航位推算等）以及全球导航卫星系统与无线定位组合定位技术（A-GPS 或 A-GNSS）。

（1）GPS 是最广泛使用的定位技术。当全球定位系统接收器在室内工作时，由于信号受到建筑物的影响会大大减弱，定位精度非常低，要实现像户外一样直接接收卫星导航数据和时间信息是不可能的。为了获得更高的灵敏度，需要延长在每个码延迟上的停留时间，A-GPS 定位技术为解决这个问题提供了可能性。室内定位技术使用大量相关器并行搜索延迟代码，而且还有助于实现快速定位。使用全球定位系统卫星定位的优势是覆盖面大，并且定位导航信号免费。缺点是定位信号达到地面时减弱，不能穿透建筑物，而且定位终端成本高。

（2）红外室内定位技术。红外室内定位系统的定位原理是红外发射器发射出经过调制的红外线，通过室内安装的红外传感器接收红外信号进行定位。虽然红外线具有较高的室内定位精度，但由于光线不能通过障碍，红外射线只能视距离传播。直线距离和传输距离短两个主要缺点使得红外室内定位效果很差。当发射器放在在口袋或有墙壁和其他障碍物遮挡时，该定位系统就不能正常工作，需要在每个房间、走廊安装接收天线，因此成本变得更高。因此，红外室内定位技术只适合短距离定位，并容易被荧光灯或房间光线的干扰，限制了定位的精确性。

（3）超声波定位技术。超声波测距主要采用超声波反射测距的方法，通过三角定位算法确定物体的位置，即发射超声波并接收被测物体产生的回波，根据回波与发射波的时差测量距离，有的则使用单向测距方法。超声波定位系统可以由很多应答器和一个主测距仪

组成，主测距仪是放置在被测物体上，在计算机的指令信号的作用下向固定位置的应答器发送同频率的无线电信号，应答器接收到无线信号后在同一时间向主测距仪发射超声波回波信号，从而得到主测距仪和应答器之间的距离。当主测距已收到三个或三个以上不在同一直线上的应答器反射的回波后，就可以根据相关计算确定被测物体的二维坐标位置。超声室内定位技术的精度较高，且结构简单，但超声波易受到多径效应和非视距传播的影响，同时也需要大量的硬件基础设施，成本太高。

（4）蓝牙技术。蓝牙技术通过测量信号强度对位置进行定位。这是一个短距离、低功耗的无线传输技术，内部安装适当的蓝牙局域网接入点，将网络配置成多用户网络连接方式，并确保蓝牙局域网接入点总是网络的主要设备，从而可以获得用户的位置信息。蓝牙技术主要应用在小范围内的定位，如大厅或仓库。

蓝牙室内定位技术最大的优点是体积小，易于集成在掌上计算机、个人计算机和移动电话内，所以很容易推广。从理论上说，只要用户持有一个集成蓝牙功能的移动终端，只要开启设备的蓝牙功能，蓝牙室内定位系统就可以进行位置定位。采用蓝牙室内定位装置的优点是容易发现设备，并且信号传输不容易受到视距的影响。其缺点是蓝牙器件和设备价格昂贵，且对于复杂的空间环境，蓝牙系统稳定性稍差，易受噪声信号干扰。

（5）射频识别技术。射频识别技术利用射频方式进行非接触的双向交换数据，以实现其目标识别和定位。这一技术的有效作用距离短，通常最长为数十米。但是，它具有几毫秒厘米级的定位精度，并且传输范围大，成本低。同时，由于其优点如非接触和非视线，有望成为首选的室内定位技术。目前，射频识别研究的热点和难点在于建立理论传播模型，如何保护用户的隐私和安全。其优点是体积较小，成本较低，缺点是有效作用距离小，没有通信能力，不易与其他系统的集成。

（6）超宽带技术。超宽带技术是一种全新的通信新技术，与传统通信技术有很大的不同。它不需要使用传统的通信体制中的载波，而是通过发送和接收纳秒或低于纳秒的一个非常窄的脉冲来进行数据传输，具有 GHz 的带宽。超宽带可用于精确室内定位，如战场上的士兵的位置，机器人运动跟踪等。

超宽带系统与传统的窄带系统相比，穿透力更强，功耗更低，多径效应影响不明显，安全更性高，系统结构简单，能提供精确的定位精度。因此，超宽带技术可以应用于室内静态或移动的物体，以及跟踪和导航，并能提供非常精确的定位精度。

（7）Wi-Fi 技术。无线局域网（WLAN）是一种新的信息获取网络平台，可以在广泛的应用领域内实现复杂的大规模的定位、监测和跟踪任务，网络结点自定位是大多数应用的基础和前提。目前流行的无线网路定位是无线局域网 IEEE 802.11 系列标准的一种定位解决方案。该系统使用的经验测试和信号传播模型组合的方式，容易安装，需要很少的基站，可以采用相同的底层无线网络结构，系统精度较高。

（8）ZigBee 技术。是一种新的短程、低速率无线网络技术，介于射频识别技术和蓝牙技术之间，也可以用于室内定位。它有自己的无线电标准，在数千个微小的传感器之间相互通信以实现定位。这些传感器只需要很少的能量，以接力的方式通过无线电波将数据从传感器传到另一个，因此其通信效率很高。ZigBee 最显著的特点是它的低功耗和低成本。

无论 GPS 定位技术还是无线定位技术都有其局限性。室内定位技术未来的发展趋势是卫星导航技术和无线定位技术相结合，发挥各自的优势，以提供更好的精度和更快的响应速度，并且覆盖范围广泛，可以实现无缝、精确定位。

2.6　典型卫星定位系统

各国都在加紧开发自己的卫星定位系统，如大家熟知的美国的 GPS，欧洲的“伽利略”卫星定位系统，俄国的“格洛纳斯”卫星定位系统，中国的“北斗”卫星定位系统。目前，GPS 是世界上最常用的卫星导航系统。本节将重点介绍 GPS 卫星导航系统。

（1）GPS 功能

GPS 定位系统简称为“球位系”，是美国陆海空三军 20 世纪 70 年代联合研制的新一代空间卫星导航定位系统。其主要目的是为陆、海、空三大领域提供实时、全天候和全球性的导航服务，并用于情报收集、核爆监测和应急通信等一些军事目的，也是美国国家安全和全球战略的信息服务和管理的重要组成部分。

（2）GPS 组成

GPS 定位系统由空间卫星、地面监控设备和用户设备（GPS 接收机）三部分组成，三者有各自独立的功能和作用，但又是有机的组合在一起而成为缺一不可的整体部分。其关系如图 2-17（a）所示。

空间卫星部分：由 24 颗工作卫星组成，包括 21 颗工作卫星和 3 颗备用卫星，均匀分布在 6 个轨道上。卫星的这种分布，保证了在地球上任何地点、任何时候都能见到 4 颗以上的卫星，并能保持良好定位解算精度的几何图形（DOP）。在时间、空间上提供了连续导航定位能力。

地面监控部分：负责监控 GPS 的工作，包括 1 个主控站、3 个注入站、5 个监控站。主控站位于科罗拉多空军基地，用来收集监控站的跟踪数据，计算卫星轨道和钟差参数，并将这些数据发送至各注入站，同时诊断卫星的工作状态并对其进行调度。注入站的主要功能是将主控站发送来的卫星星历和钟差信息注入卫星。监控站的作用，对所收到的卫星进行连续的 P 码伪距跟踪测量，并将观测结果传送到主控站。

用户设备部分：主要由各种 GPS 接收机组成，其作用就是接收、跟踪、变换和测量

GPS 信号。按工作原理可分为码相关型、平方型、混合型、干涉型接收机；按用途可分为导航型、测地型、授时型接收机；按载波频率可分为单频、双频接收机；按接收信道数分为多信道、序贯信道、多路多用通道接收机。对于研究地壳板块运动的用户，由于对测量精度的要求，通常采用双频多通道混合型测地接收机。用户的导航终端界面如图 2-17（b）所示。

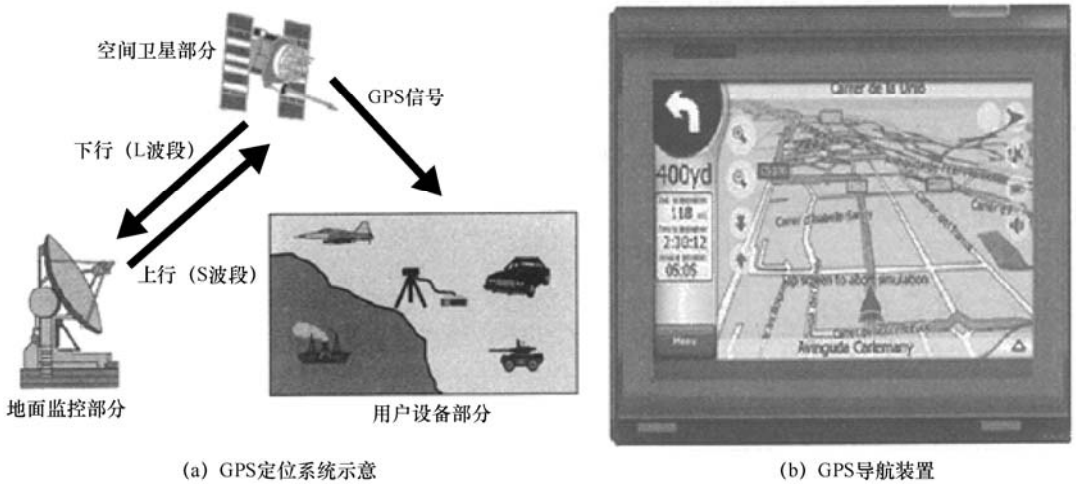


图 2-17　GPS 定位系统

（3）GPS 特点

GPS 的主要特点包括高精度、全天候、高效率、多功能、操作简便、应用广泛等。

定位精度高：实践已经证明，GPS 相对定位精度在 50km 以内可达 10-6；100～500km 可达 10-7；1000km 可达 10-9。在 300～1500M 工程精密定位中，1h 以上观测的其平面位置误差小于 1mm，与 ME-5000 电磁波测距仪测定的边长比较，其边长误差最大为 0.5mm，校差中误差为 0.3mm。

观测时间短：随着 GPS 的不断完善，软件的不断更新，目前 20km 以内相对静态定位，仅需 15～20min；快速静态相对定位测量时，当每个流动站与基准站相距在 15km 以内时，流动站观测时间只需 1～2min，然后可随时定位，每站观测只需几秒。

（4）GPS 应用

GPS 在导航、跟踪、精确测量等方面都有很广泛的应用。定位导航是人们对 GPS 最常用的方法，GPS 已是汽车、船舶、飞机等运动物体的基本配置，其界面是人们最熟悉的图像。日常它用于对船舶远洋导航和进港引水，飞机航路引导和进场降落，汽车自主导航定位，地面车辆跟踪和城市智能交通管理等。在日常安全方面对于警察、消防及医疗等部门

的紧急救援、追踪目标和个人旅游及野外探险的导引等，GPS 都具有得天独厚的优势。在日常生活中，GPS 还可用于人身受到攻击危险时的报警，特殊病人、少年儿童的监护与救助，生活中遇到各种困难时的求助等。

在军事领域，GPS 也已从当初的为军舰、飞机、战车、地面作战人员等提供全天候、连续实时、高精度的定位导航，扩展到成为目前精确制导武器复合制导的一种重要技术手段。

（5）GPS 前景

由于 GPS 技术所具有的全天候、高精度和自动测量的特点，作为先进的测量手段和新的生产力，已经融入了国民经济建设、国防建设和社会发展的各个应用领域。

美国政府宣布在保证美国国家安全不受威胁的前提下，取消选择可用性（SA）政策（美国国防部为减小 GPS 精确度而实施的一种措施），GPS 民用信号精度在全球范围内得到改善，利用 C/A 码进行单点定位的精度由 100m 提高到 200m，这将进一步推动 GPS 技术的应用，提高生产力、作业效率、科学水平以及人们的生活质量，刺激 GPS 市场的增长。

2.7　物体间时间同步机制与方法

定位和时间同步技术是报告事件位置、跟踪目标、地理路经、网络管理等系统功能的基本技术。物理时间用来表示人类社会使用的绝对时间，逻辑时间表达事件发生的顺序关系，它是一个相对的概念。对于物联网这种环境，各传感结点之间距离无法实现设定，空间距离有时可能较远。从控制技术来看这里最常采用的技术是分布式控制，其特征是一种分布式系统。因此通常需要一个表示整个系统时间的全局时间，这个时间根据需要可以是物理时间或逻辑时间。因此，时间同步对于无线传感网是十分重要的。因为，不同结点的传感器都有自己的本地时钟，各单元内的时间振荡器之间存在着偏差，若要各结点达到时间同步，则必须在时钟上统一。以此，时间同步称为分布式系统中的关键技术之一。因为，传感器网络在能量、价格和体积等方面的约束，使得复杂的时间同步机制不适用于它，需要修改或重新设计时间同步机制来满足传感器网络的要求。

（1）时钟同步

时钟同步对任何分布式系统而言都是很重要的，无线传感器网络中许多算法或协议也需要结点间的时钟同步作为支撑。在无线传感器网络的应用中，传感结点采集的数据如果没有空间和时间信息是无任何意义的。准确的时间同步是实现传感器网络自身协议的运行、数据聚集、TDMA 调度、协同休眠、定位等的基础。例如，多个传感器联合来探测一个运动目标，如车辆或者坦克的轨迹，每个传感器将它观测到的位置和时间返回到处理中心，如果这些时钟不事先同步，那么将无法判断观测到的位置的时序，从而无法计算出轨迹。

在链路层采用时隙分配的 MAC 协议时，结点间如果不能保持时钟同步，会造成时隙混乱无法有效利用带宽资源。

对于无线传感器网络而言，结点的本地时钟的频率是由晶振和计数寄存器构成的，每出现一定数量的振荡脉冲，寄存器值就增加 1，访问该寄存器便可知当前时间。在本地时钟基础上，可构造不同类型的软件时钟。由于结点采用的晶振性能差异较大，且晶振频率受电压、温度及使用时间等多种因素的影响，使晶振的实际工作频率与出厂标定值有差异，导致结点之间时钟不同步。

1）速率恒定模型。

对于速率恒定模型，$r(t)\dfrac{\mathrm{d}C(t)}{\mathrm{dt}}$=常数，即晶振频率为常值。当要求的时钟同步精度远低于频率变化引起的偏差时，该模型的假设是合理的。

2）漂移有界模型。

通常情况下，时钟速率 $r(t)$ 在一定范围内波动，即 $1-\rho \leqslant r(t) \leqslant 1+\rho$，其中，$\rho$ 为时钟漂移。

3）漂移变化有界模型。

时钟漂移的变化 $\xi(t)\dfrac{\mathrm{d}\rho(t)}{\mathrm{d}t}$ 是有界的，即 $-\xi_{\max} \leqslant \xi(t) \leqslant \xi_{\max}$。对于结点 i 和 j，用 $C_i(t)$、$C_j(t)$ 表示它们在 t 时刻的时间值。若采用速率恒定模型，$C_i(t)$ 可表示为 $C_i(t)=at_i+b_i$。由此可知，任意两个结点 i 和 j 的时钟满足如下线性关系：

$$C_i(t)=a_{ij}C_j(t)+b_{ij} \tag{2-16}$$

式中，a_{ij} 和 b_{ij} 分别为相对漂移与相对偏移。

当两个结点的时钟保持同步，即 $C_i(t)=C_j(t)$ 时，$a_{ij}=1$，$b_{ij}=0$。因此，对于采用速率恒定时钟模型的场合，时钟同步就是对 (a_{ij},b_{ij}) 进行估计，这样，两个结点在新的时刻便保持时钟同步。

时钟同步算法执行周期是系统的关键之一，以此选择合适的时钟同步算法执行周期十分重要。过于频繁地执行时钟同步算法会占用一定的时间和带宽资源，特别是控制报文开销；但时钟同步算法执行的时间间隔过长时，时钟偏差不能满足相关应用对时钟同步的精度要求，进而影响相关协议和应用的性能。重要的是当结点间时钟偏差不满足协议和应用要求时，才执行时钟同步算法。下面推导时钟同步间隔与同步误差、时钟漂移率的关系。若 f 为晶振工作频率（单位：MHz），ρ 为时钟漂移率，f_+、f_- 分别为晶振的最大和最小工作频率，则

$$f_+=(1+\rho)f \tag{2-17}$$

$$f_-=(1-\rho)f \tag{2-18}$$

则结点间时钟周期偏差最大值为

$$T_{\Delta}=T_{-}-T_{+}=\frac{1}{f_{-}}-\frac{1}{f_{+}}$$
$$=\left(\frac{1}{1-\rho}-\frac{1}{1+\rho}\right)\frac{1}{f}=\frac{2\rho}{(1-\rho^{2})f}\approx\frac{2\rho}{f} \tag{2-19}$$

累计同步误差为

$$t_{\Delta}=t_{\text{sync}}T_{\Delta}f \tag{2-20}$$

式中，t_{sync} 为两次时钟同步的时间间隔。

因此，

$$t_{\text{sync}}=\frac{t_{\Delta}}{T_{\Delta}f}\approx\frac{t_{\Delta}}{2\rho} \tag{2-21}$$

时钟同步评价在无线传感器网络中的时钟同步算法评价指标包括定量和定性两个方面。其中，定量指标包括同步精度、计算复杂度、协议收敛时间等；定性指标包括可扩展性、能量有效性、容错等。

在这些过程中，必须注意以下几个方面的问题：同步精度决定了结点间以某一基准进行时间同步的偏差；计算复杂度决定了算法在选定参与转发数据帧的结点所发送的分组数的量级；协议收敛时间决定了时间同步算法在全网内完成一个轮回所用时间，即从网络时间发生变化到网络上所有的相关结点都得知这一变化，并且相应地完成同步算法所需要的时间；系统的可扩展性决定了在传感器网络应用中，结点随机分布，因此分布密度通常不均匀，时钟同步机制必须能够适应这种网络范围和结点分布密度的变化；能量保障性决定了系统的生命周期，必须最小限度且均匀地使用结点能量。为了减少能量消耗，应使网络时钟同步的交换信息尽可能得少，网络通信和计算处理的能耗应可预知，时钟同步机制应该根据网络结点的能量分布，均匀地使用网络结点的能量来达到能量的高效使用。

（2）传统的时钟同步

在传统网络中，已经提出了多种网络同步机制，C/S 模式是主要的时钟同步模式。客户端产生时钟同步请求消息，服务器回应时钟同步应答消息，通过测试这两个消息的发送和接收时间来估计两者的时间偏差，获得相对较精确的时钟同步。采用上述思想的典型例子就是网络时间协议 NTP，被因特网用做网络时钟同步协议，NTPv4 精确度已达到毫秒级。实现方案是在网络上指定若干时钟源服务器，为用户提供授时服务，并且这些服务器之间能够相互比较校正，以提高准确度。NTP 协议采用层次型树型结构，整个体系结构中有多棵树，每棵树的父结点都是一级时间基准服务器。NTP 协议要将时间信息从这些一级时间服务器传输到分布式系统的二级时间服务器成员和客户端，第三级时间服务器从第二级服务器获得时间信息，以此类推，服务器级数越小，越接近一级服务器，时间就越准确。由于 NTP 协议设计对象为因特网和计算机，设计重点为协议的可靠性和同步精度。该协议要求能够始终占用 CPU 资源，以便它可以执行连续的操作，使时钟一直保持同步，没有考虑

能耗和计算能力问题，无法直接用于无线传感器网络中。

在无线传感器网络应用中，结点对功耗有着严格的要求，并且要求尽可能保持较小的外形尺寸和低廉的成本使其能够被大量部署，其部署环境经常是常人难以接近的恶劣环境，这使得部署后的维护通常是不可能的。显然将 GPS 和 NTP 用于无线传感器网络的时间同步是不可取的。分布式系统中对时间同步也有大量研究，但这些方法都没有考虑传感器网络的特点，需要较大的资源开销，所以不适合传感器网络的时间同步。鉴于时间同步在无线传感器网络应用中的基础性作用，必须研究适用于无线传感器网络的时间同步算法。

（3）时钟同步方法

时间同步方法在系统中十分重要，它决定了传感网各点的协调一致的准确度，解决这个问题依靠的是时间同步协议。通常时间同步协议可分为两类，即发送与接收的同步和接收与接收的同步。最基本的方法是发送者在报文中嵌入发送时刻，而接收者则记录下报文接收到的时刻。利用这些时间信息可估算出收发双方的时间偏差，通过对时间偏移的补偿，实现收发双方的时间同步。

接收与接收的同步协议，与发送与接收的同步协议不同。接收与接收的同步协议是为了多个接收者的同步。结点之间为了达到同步需要交换各种各样的消息，受信道质量、结点工作环境和结点配置等因素的影响，同步消息在传输过程中的延迟具有不确定性，这是无线传感器网络时间同步的主要挑战之一。同步消息从发送方要依次经过发送时间延迟、发送方 MAC 访问时间延迟、物理层传播延迟、接收方 MAC 屡接收延迟，接收方应用程序层延迟，最终才能到达接收方的应用程序层。

采取的主要方法有：发送时间是用来产生同步消息并向 MAC 层提交发送请求，该过程的持续时间取决于当前处理器的载荷和操作系统的负担，因而具有不确定性；典型值为 0～100ms。访问时间用来等待信道空闲的时间，依赖于网络的流量，也具有不确定性；典型值为 10～500ms。传输时间是用来传输同步消息的时间，取决于消息的长度和无线电波的传输速度，具有确定性；典型值为 10～20ms。传播时间是为了同步信息离开发送方至接收方的时间，取决于两者的距离，具有确定性，但该时间通常可忽略。典型值为<1μs（距离<300m）。接收时间与发送方的传输时间特性相同，且在同步消息传输过程中两者重叠，典型值为 10～20ms。接收处理时间是接收方用来处理同步消息的时间，与发送时间的特性相同，典型值为 0～100ms。因此，一般在发送方 MAC 层后对同步消息添加时间戳，接收方在接收时间后添加时间戳，减少发送时间、访问时间和接收处理时间延迟的不确定性给同步精度带来的影响。

（4）硬件支持的时钟同步

在结点上安装 GPS 接收机，实现结点时钟与 UTC 同步是典型的额外硬件支持的同步方法。虽然 GPS 的时钟同步精度可达纳秒级，但 GPS 能耗大且某些情形下无法接收 CPS

信息，不适合大规模的无线传感器网络应用。

压控晶体振荡器（VCO）时钟同步机制利用参考时钟与结点本地时钟的偏差作为 PI 控制器的输入，控制器的输出为控制电压，用来控制 VCO 的输出频率。当本地时钟与参考时钟一致时，PI 控制器的输出为常值，VCO 的振荡频率也为常值。

（5）广播式时钟同步

“第三方广播”的方式参照结点利用物理层广播周期性地向网络中其他结点发送参照广播。在广播域中的结点，用自己的本地时钟记录各自的包接收时间。然后相互交换记录的时间信息。由于 RBS 采用接收者之间进行同步的方法，在关键路径中排除了发送方的发送时间和访问时间对同步精度造成的影响，使得广播同步机制得到比双向成对同步好得多的同步精度。RBS 的缺点是对网络有一定的要求，不适合点对点通信的网络。结点间交换本地时间也需要额外的消息开销，对于由 n 个结点构成的单跳网络，需要 $0(n^2)$的消息交换。当 n 很大时，消息交换开销和结点的计算开销也非常大，扩展性差。另外，RBS 实现的是接收结点之间的时钟同步，未实现与参考结点的同步。DMTS 算法引入时间戳（标记参考结点发送同步消息时刻）的概念，参考结点向区域内的结点广播带有时间戳的同步消息，接收结点通过精确地测量从发送结点到接收结点的单向时间延迟，结合发送结点中的时间戳计算时间调整值。这就避免了 RBS 算法中需要结点之间交换时钟信息且无法与参考结点的时钟保持同步的缺点。

商品推广解决方案技术所提供的算法没有估计时钟的频率漂移，时钟保持同步的时间较短；也没有消除时钟刻度的影响，因而其精度不高，不适用于定位要求高精度同步的场合。

FTSP 图像处理软件中的算法，也是使用单向广播消息实现发送结点与接收结点之间的时间同步，但是算法的具体实现与商品推广解决方案有所不同。FTSP 图像处理软件彩采用参考结点多次广播带有发送时间戳的同步消息的方法，使每个结点获得多个属性对，通过集中式线性回归法对时钟的相对漂移和相对偏移进行估计。为了提高时间戳标记的精度，FTSP 算法通过对收发过程时延的分析，进一步降低了时延的不确定性。

（6）双向时钟同步

双向成对同步典型代表有 TPSN、Tiny-Sync/Mini-Sync，结点 i 在 T_1 时刻向结点 j 发送同步消息 SYNC_MSG，结点 j 用自身的时钟记录同步消息到达的时刻 T_2，则 $T_2 = T_1 + D + d$，其中，D 是消息传输的时间；d 是结点之间的时钟偏移。然后，在 T_3 时刻结点 j 向结点 i 返回一个包含 T_2 与 T_3 的应答消息 ACK_MSG，结点 i 在 T_4 时刻收到该应答消息，则 $T_4 = T_3 + D - d$。若在发送同步消息和应答消息过程中的传输时间相同，通过式 $\begin{cases} d = \dfrac{(T_2 - T_1) - (T_4 - T_3)}{2} \\ D = \dfrac{(T_2 - T_1) + (T_4 - T_3)}{2} \end{cases}$ 可计

算时钟偏移和传输时间。

传感器网络时间同步（TPSN）算法是双向成对同步方法，分为层次发现段和同步阶段两个阶段。

层次发现阶段的目的是在网络中产生一个分层的拓扑结构，并使每个结点都赋予一个层次号。同步阶段的核心就是结点间成对的消息交换。该阶段由根结点的 time_svnc 包发起，当接收到这个包，第一层的结点发起与根结点的双向消息交换。在发起消息交换之前，为最小化无线信道冲突，每个结点都要等待一个随机时间。一旦接收到根结点的应答消息，可用上述公式计算它们之间的偏移和传播延迟，并调整自身时钟到根结点的时钟。第二层结点监听到第一层的一些结点与根结点的通信后，发起与第一层结点的双向消息交换，再一次需要等待一个随机时间以确保上层结点完成同步。这个过程最终使所有结点都与根结点同步。在该过程中，下层结点不可避免地会与多个上层结点同步。

TPSN 算法的缺点是一旦根结点失效，就要重新选择根结点并重新进行上述两个过程，增加了计算量和能量开销。同步阶段所用时间随结点数目的增加而线性增加。协议要求网络构造层次结构，使得它不适合高度移动的结点。

但同步误差随着包含时间戳的消息路径的跳数的增加而增加，在稀疏网络中跳数一般较多，这明显影响了同步精度。萤火虫同步技术对耦合延迟、耦合强度、耦合性质、初始相位、网络拓扑等隐私很敏感。虽然在两个振荡器的同步收敛性研究上取得了一定进展，但无论是理论研究或模拟研究，研究者在某些结论上还不能达成一致。但有一点可以认同：在实际系统中，基于萤火虫的同步技术会取得一定误差范围内的同步。

上述算法都可以扩展到多跳情形，但同步精度与单跳情形相比略有降低，且随着跳数的增加，误差也会增加。值得注意的是，双向成对时钟同步需要两个结点间分别交换消息，这就意味着在共享信道时由于 MAC 协议的不合理会导致信道冲突。

（7）锁相环同步

考虑到无线传感器网络中由于结点和链路失效等因素导致拓扑结构动态变化的特点，以及为均衡能量损耗、延长网络生命周期而采用拓扑控制等系统性优化能耗的方案对网络带来的影响，沿用 FTSP 中根结点的选取和维护方案，着重讨论广播域内单跳同步机制与原理，在此基础上扩展到整个网络的多跳机制是较为直接和方便的。在一个广播域内，时钟参考结点（时标）周期性广播同步分组，分组中携带了时标结点的本地时钟，为避免广播分组在发送、访问信道和接收过程中由于系统和信道状态的不确定性因素可能引起的误差，采用在 MAC 层加盖时戳的方案。收到同步分组的结点容易得到两个时钟间的差，FTSP 和 DMTS 直接用差值进行了偏移补偿。如果能通过分析这个差值时间序列，得到两个时钟相对漂移的信息，一次完成偏移和漂移补偿，则这样的时间同步算法会更有效率。因为它

不会再像 FTSP 那样，为了进行线性回归处理而维护大量的历史数据。为此，需要设计一个简单的滤波器来递推估计差值序列的变化，进行相应的校正。这一新机制称为广播校正同步机制。

2.8 时间同步协议

根据同步实现的机制，时间同步协议可以分为三大类：基于接收方—接收方机制的算法，如 RBS，基于成对机制的算法，如 TPSN 和 Mini-Sync 协议和 Tiny-Sync 协议，基于 Sender-Receiver 机制的时间同步协议，如 FTSP 等。

2.8.1 基于 Receiver-Receiver（接收方—接收方）机制的时间同步协议

参考广播同步（RBS）是由 J. Elson 等人提出使用无线数据链路层的广播信道特性，实现接收结点之间时间同步的一种算法，在 RBS 算法中引入了接收方—接收方（Receiver-Receiver）机制。在该算法中，参考结点发送消息给邻近结点，这个参考消息不包含时间戳。反之，接收结点将到达时间用来作为参考，与本地时钟作对比。该算法不是使发送者和接收者同步，而是使接收者之间同步。其基本思想是：一个参考结点周期性的向邻居结点发送参考广播消息，每个邻居结点记录并缓存报文的到达时间。任何结点之间需要同步时，必须交换缓冲区中存储的时间信息，两个时间的差值即为两个接收结点之间的时间差。可以使用最小方差线性拟合估算两个结点之间的初始相位差和频率差值，以便获得两结点间的时间转换函数，其中一个接收结点根据时间差，调整它的本地时间。因此，RBS 算法通过时间转换函数实现了结点间的时间同步。其主要优点是可以排除发送时延的不确定性，同步精度高（见图 2-18）。其误差的主要来源是传输时间和接收时间的不确定性，传输时间在射频范围很小的情况下被认为是微不足道的。其缺点是误差随跳计数的增加而增加，不适合多跳网络，能量消耗过大，不适合有限能源的应用。

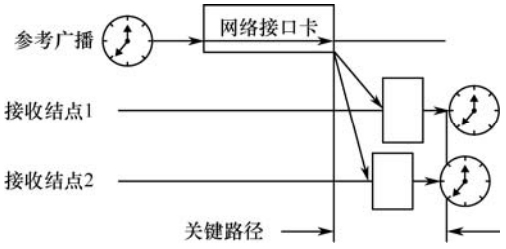


图 2-18　RBS 协议的基本原理

2.8.2 基于成对机制的时间同步协议

下面介绍两种典型的基于成对机制的时间同步协议。

（1）TPSN（Timing-sync Protocol for Sensor Networks）算法

TPSN 的设计类似于传统网络中的 NTP，采用发送者与接收者之间成对同步的工作方式，结点之间通过双向的消息交换实现结点间的时间同步。TPSN 的同步过程分为两个阶段：层次发现阶段（level discovery phase）和同步阶段（synchronization phase）。

第一阶段的目的是建立分层的网络生成树，每一个结点都有一个层次级别，树的根结点作为时钟源结点，它的层次为 0。在层次发现阶段的开始，根结点广播一个层次发现包，其中含有根结点的 ID 和层次等级。在根结点通信范围内的结点收到这个数据包，就给自己指派一个比数据包中的层次等级大一的级数。然后这些结点用它们自己的 ID 和层次等级广播新的层次发现包。这个过程不断地进行，一直到所有的结点都有自己的等级。

第二个阶段的主要任务是结点之间的双向信息交换。层次结构建立以后，根结点通过广播时间同步数据包启动同步阶段。同步阶段最基础的一部分就是两个结点间双向的消息交换。假设在单个消息交换的很小一段时间内，两个结点的时钟偏差是不变的，传播延迟在两个方向上也是不变的。图 2-19 所示的结点 A 和结点 B 之间的双向消息交换，结点 A 在 T_1（根据本地时钟）发送同步信息包，这个包包含结点 A 的等级和 T_1，结点 B 在 T_2=（$T_1+d+\Delta$）收到这个包，其中Δ是两个结点间的时钟偏差，d 是消息的传播延迟，结点 B 在 T_3 返回确认信息包，信息包包含结点 B 的等级和 T_1，T_2，T_3，然后，结点 A 在 T_4 时刻收到确认信息包，T_4=（$T_3+d-\Delta$）能够计算出时钟漂移和传输延迟，并与结点 B 同步。

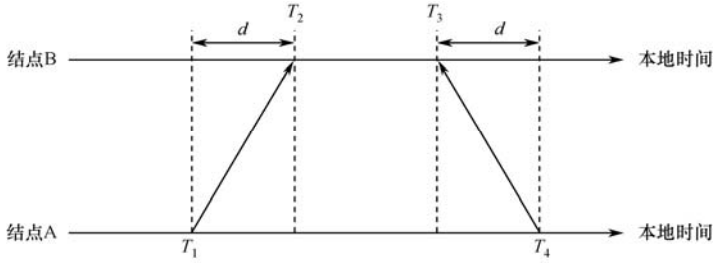


图 2-19　TPSN 同步消息交换原理

在发送时间、访问时间、传播时间和接收时间四个消息延迟组成部分中，访问时间往往是无线传输消息时延中最具不确定性的因素。为了提高两个结点间的时间同步精度，TPSN 协议只有在 MAC 层消息开始发送到无线信道的时候，才给同步消息加上时标，消除了访问时间带来的时间同步误差。TPSN 协议能够实现全网范围内结点间的时间同步，同步误差与跳数距离成正比增长。该协议的一个显著不足就是没有考虑根结点失效问题。新的传感器结

点加入网络时，需要初始化层次发现阶段，使级别的静态特性减少了算法的鲁棒性。

$$\begin{cases} \Delta = \dfrac{(T_2 - T_1) - (T_4 - T_3)}{2} \\ d = \dfrac{(T_2 - T_1) + (T_4 - T_3)}{2} \end{cases} \tag{2-22}$$

（2）Mini-Sync 协议和 Tiny-Sync 协议

Mini-Sync 协议和 Tiny-Sync 协议都是在传感器网络中形成一个层次结构，并假设每个结点的振荡器频率在特定的时间段内是恒定的，采用双向消息交换来估计结点的相对时钟漂移率和时钟偏差。假设任何两个结点的在同一时刻的时钟读数 T_1 和 T_2 是线性的，如下式：

$$T_1 = a_{12}T_2 + b_{12} \tag{2-23}$$

其中，a_{12} 和 b_{12} 分别是两个结点之间的相对时钟漂移率和相对时钟偏移，如果这两个结点已经同步，那么相对时钟漂移率就是 1，相对时钟偏差就是 0。如果结点 1 已知 a_{12} 和 b_{12} 的值，由式（2-23）就可以估算出结点 2 的时钟。为此，结点 1 发送一个探测消息给结点 2，标记发送时刻为 T_0，结点 2 接收这个探测消息，并标记接收时刻为 T_b，然后立即把消息发回给结点 1，结点 1 记录接收消息的时刻为 T_r，如图 2-20 所示。

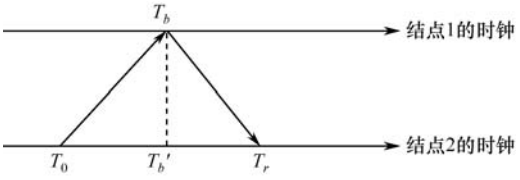


图 2-20　TS/MS 协议探测消息交换的过程

因此，结点 1 每次交换信息后都可以获得一个数据点，这个数据点由 T_0、T_b 和 T_r 组成，数据点有效地限制了变量 a_{12} 和 b_{12} 值。因为结点的时间是单调递增的，所以有以下不等式：

$$T_0 < a_{12}T_b + b_{12} \tag{2-24}$$

$$T_r > a_{12}T_b + b_{12} \tag{2-25}$$

上述测量将会重复多次，每次探测都会返回一个新的数据点，通过式（2-24）和式（2-25）对 a_{12} 和 b_{12} 的范围产生新的约束。至少需要两个数据才能够计算出 a_{12} 和 b_{12} 的上下界，图 2-21 表示结点 1 和结点 2 的时间线性关系与参数 a_{12} 和 b_{12} 取值的约束范围，两条线的斜率对应于 a_{12} 的最大值 $\overline{a_{12}}$ 和最小值 $\underline{a_{12}}$，截距对应 b_{12} 的最大值 $\overline{b_{12}}$ 和最小值 $\underline{b_{12}}$，a_{12} 和 b_{12} 的取值为上述极值的平均值。结点 1 会收集多个数据点，当接收到一个新的数据点时，将这个数据点与现有的数据点比较，若新的数据点计算出的误差大于以前数据点计算的误差，则丢弃新的数据点；否则，采用新的数据点并丢弃现有数据集中的某个数据点，结点只保存能够提供最好曲线的数据点。当然，如果结点 2 不能立即发回消息，式（2-24）和式（2-25）同

样成立。

Tiny-Sync 协议使用最少的数据点，降低了能量的消耗，同时也降低了同步的精度。Mini-Sync 协议则使用较多的数据点以实现较高的同步精度，但是巨大的通信量导致能量消耗增加。Mini-Sync 协议是 Tiny-Sync 协议的扩展，解决了保留可能被 Tiny-Sync 协议忽略的，却可能在以后提供较好约束的数据点的问题。如图 2-22 所示，Tiny-Sync 协议在收到数据点 $(A_3 - B_3)$ 之后，数据点 $(A_1 - B_1)$，$(A_3 - B_3)$ 被存储，而 $(A_2 - B_2)$ 被丢弃，当下一个数据点 $(A_4 - B_4)$ 能够与 $(A_2 - B_2)$ 产生更好的估计时，数据点 $(A_2 - B_2)$ 已经被删除，因此可能会错过最优的结果。考虑到上述问题，可以采取这样的对策，对于任何约束数据点 A_j，如果满足

$$m(A_i, A_j) \leqslant m(A_j, A_k)\ ,(1 \leqslant i < j < k)$$

那么，这个数据点可以丢弃。这两个协议通过很低的计算、存储和通信成本，提供了相对时钟漂移率和时钟偏差的上下界。然而，它们同样使用分层的网络结构，因此不能适应网络拓扑结构发生的情况。

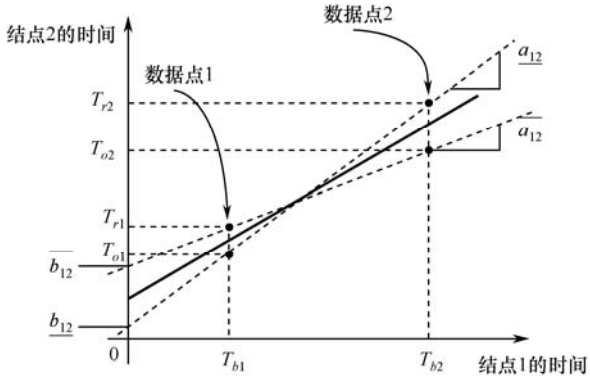


图 2-21　a_{12} 和 b_{12} 的上下界

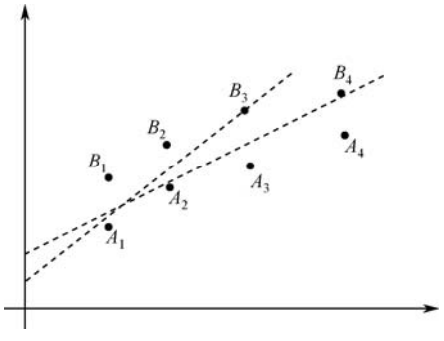


图 2-22　Tiny-Sync 协议中丢失数据的情况

2.8.3　基于 Sender-Receiver（发送—接收方）机制的时间同步协议

基于 Sender-Receiver 机制的时间同步算法的基本原理是：发送结点发送一个包含本地时间戳的时间同步消息，接收结点记录本地接收时间，并将其与同步消息中的时间戳进行比较，调整本地时钟。基于这种方法提出的时间同步算法有以下两种。

（1）DMTS 算法

延迟测量时间同步算法（Delay Measurement Time Synchronization，DMTS）是基于同步消息在传输路径上所有延迟的估计，实现结点间的时间同步。实现策略是牺牲部分精度换取较低的计算复杂度和能耗，是一种轻量的能量有效的时间同步算法。

基本原理：选择一个结点作为时间主结点广播同步时间消息。所有接收结点测量这个时间广播消息的延迟，设置自己的时间为接收到消息携带的时间加上这个广播消息的传输延迟，这样所有接收到消息的结点都与主结点进行时间同步。发送结点和接收结点的时间延迟 t_d 可由式（2-26）得出：

$$t_d=nt+(t_2-t_1) \tag{2-26}$$

其中，nt 为发送前导码和起始字符所需的时间，n 为发送的信息位个数，t 为发送一位所需时间；t_1 为接收结点在消息到达时的本地时间；t_2 为接收结点在调整自己的时钟之前的那一时刻记录的本地时间，（t_2-t_1）是接收处理延迟。

（2）FTSP 算法

泛洪时间同步协议（Flooding Time Synchronization Protocol）由 Vanderbilt 大学 Branislav Kusy 等提出，目标是实现整个网络的时间同步并且误差控制在微秒级。该算法与 TPSN 类似，但改进了 TPSN 的不足。它与 TPSN 结构上的相似之处是都有一个根结点，其他结点都与根结点同步。算法采用单个广播消息实现发送结点与接收结点之间的时间同步，具体步骤如下。

在完成 SYNC 字节发送后给消息标记时间戳 t 并发送出去，SYNC 字节类似于 DMTS 算法中的前导码和起始字符。时间戳 t 为当前时间减去包含时间戳 t 的消息数据部分的发送时间，消息数据部分的发送时间可通过数据长度和发送速率得出。

接收结点记录 SYNC 字节最后到达时间 t_r，并计算位偏移。收到完整消息后，接收结点计算位偏移产生的时间延迟 t_b，可通过偏移位数与接收速率得出。

接收结点调整本地时钟与发送结点同步，两者时钟偏移量为：offset=t_r-t_b-t。FTSP 协议针对大规模多跳网络而设计，支持网络拓扑结构的变化；根结点通过动态、周期的选举产生，对结点或链路的失效有鲁棒性；通过采用 MAC 层时间戳和线性回归偏差补偿弥补了相关的错误源，精确度较好。

2.8.4 典型时间同步协议的比较

上述几种同步协议是现有的最具代表性的同步方法，其他的同步方法大都是借鉴这几种协议，根据各自的需求做出改进而得到的。这些时间同步协议各有所长，协议是基于应用的，因此对于具体的应用应当根据协议的特点，选择合适的协议。基于无线传感器网络时间同步协议的同步精度、同步范围、网络的拓扑结构和扩展性以及通信成本等方面对以上几种协议进行总结比较，见表 2-5。由表 2-5 可以得出，与另外几种协议相比，发送方—接收方模式的 FTSP 在同步精度、通信开销、扩展性、鲁棒性和能耗方面都有着明显的优势。由于网络拓扑结构的影响，新加入的结点或者结点失效，对其他几个协议的扩展性和鲁棒性都会造成影响，尤其是 Tiny-Sync/Miny-Sync 和 TPSN 协议，结点的加入或者离开对现有的分层结构影响很大，如果网路中某个结点失效，将会引发连锁反应，导致这个失效结点的所有后继结点的时间无法同步。

表 2-5 典型时间同步协议的比较

协议 / 性能	RBS	TPSN	Tiny-Sync/Miny-Sync	FTSP
消息延迟	传播延迟和接收延迟	接收时延	传输时延、传播时延和接收时延	传播时延
扩展性	较差	很差	很差	好
同步范围	子网	全网	子网	全网
同步精度	一般	较高	低	高
复杂度	中等	中等	高	中等
通信成本	每个同步周期发送 1.5 个同步信息	每个同步周期发送两个同步信息	每个同步周期发送两个同步信息	每个同步周期发送 1 个同步信息
网络的拓扑结构	多个参考结点，其他结点在各自的参考域内同步	分层树结构	分层结构	只有一个 ID 最小的结点作为参考结点

第 3 章　物体信息传输网络与要素控制

3.1　有线与无线网络的选择

随着各种广域网、局域网与公用分组交换网的发展，各生产商纷纷发展各自的网络系统，网络结构与协议标准等技术的国际化，推动了网络技术的迅速发展。互联网作为全球信息网，从有线网络到无线网络技术，基于光纤通信技术的宽带城域网，以及移动网络计算、网络多媒体计算、网络并行计算、网格计算与存储区域网络等，使互联网技术日趋成熟。

互联网和物联网的接入主要有两种类型：有线接入与无线接入。

1）有线接入：是指计算机通过网卡接入局域网，然后再接入地区主干网和国家或国际主干网，最终接入到互联网。常用的接入装置有两种：一种是用 ADSL 接入设备，通过电话交换网接入互联网；另一种是采用 Cable Modem 接入设备，通过有线电视网接入互联网。

2）无线接入：是采用无线网卡接入到无线局域网中，再通过小地区网接入大地区主干网，再由地区主干网接入国家或国际主干网，最后接入互联网。

物联网和传感网常用的接入方式主要是无线接入，即通过无线网卡和相应的设备，无线接入到城域网，再接入互联网。在有的环境下，物联网无线接入是采用无线自组网完成首个接入后，再通过最近的基站接入到互联网中。下面主要就无线网络作介绍。

3.1.1　无线网络的基本概念

（1）无线网络的分类

从无线网络技术的分类、分组与自组网等基础设施的角度来看，可以分为两大类：基于基础设施的无线网络和无基础设施的无线网络。图 3-1（a）为网络的分类。

（2）无线自组网（MANET）与无线传感器网络

IEEE 将无线自组网的网络定义为一种特殊的自组织、对等式、多跳、无线移动网络，

称为移动无线自组网络。无线传感器网络在军事上可以用于对敌方兵力和装备的监控，战场的实时监视，目标的定位、战场评估以及对核攻击和生物化学攻击的监测和搜索。无线传感器网络研究将涉及传感器、微电子芯片制造、无线传输、计算机网络、嵌入式计算、网络安全与软件等技术，是一个由多个学科专家参加的交叉学科研究领域。

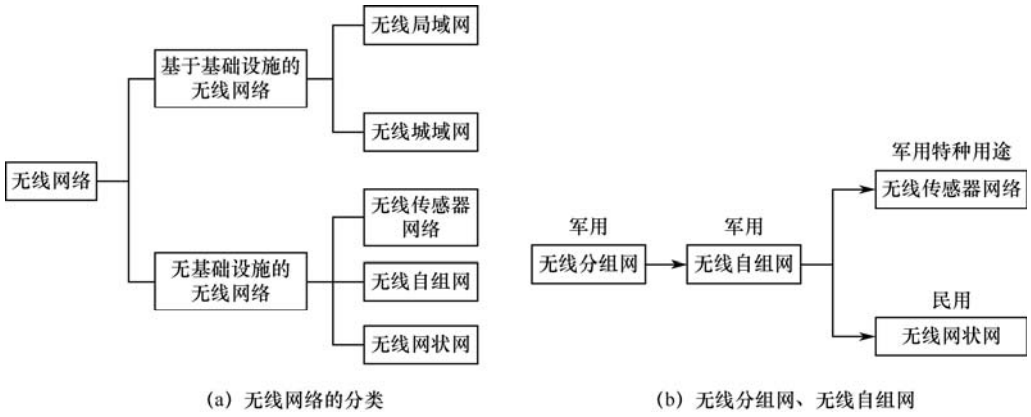


图 3-1　网络的分类

（3）无线自组网与无线网状网

无线自组网技术作为无线局域网与无线城域网等无线接入技术的一种补充，应用于互联网无线接入网中。无线自组网技术向两个方向发展：一个是向军事、特定行业发展和应用的无线传感器网络；另一个是向民用接入网领域发展的无线网状网。这些网络之间的关系如图 3-1（b）所示。

3.1.2　无线局域网与协议

（1）无线局域网的应用领域

随着无线局域网技术的发展，人们越来越深刻地认识到，无线局域网不仅能够满足移动和特殊应用领域网络的要求，还能覆盖有线网络难以涉及的范围。它们主要有以下两个方面。

1）作为传统局域网的扩充。

传统的局域网用非屏蔽双绞线实现 10Mbps，甚至更高速率的传输，使得结构化布线技术得到广泛应用。很多建筑物在建设过程中已预先布好双绞线，但是在某些特殊的环境中，无线局域网却能发挥传统局域网起不到的作用，例如在建筑物群之间、工厂建筑物之间的连接，股票交易等场所的活动结点，以及不能布线的历史古建筑，临时性的大型报告会与展览会。在上述情况中，无线局域网提供一种更有效的联网方式。

目前在多数情况下，局域网用来连接服务器和一些固定的工作站，而移动和不易于布线的结点可以通过无线局域网接入。图 3-2 给出了典型的无线局域网结构。

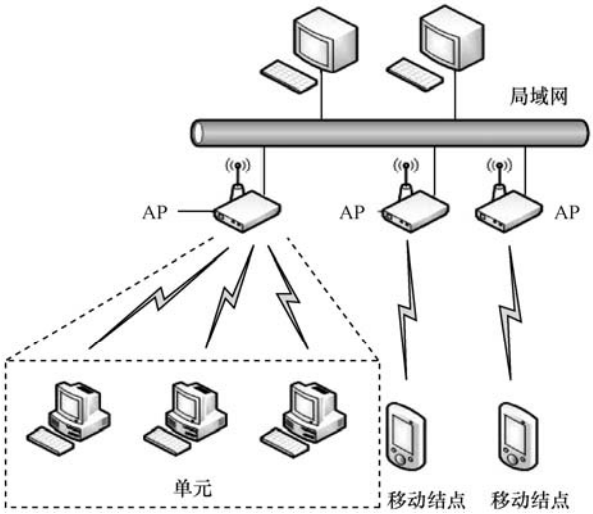


图 3-2　典型的无线局域网结构

2）特殊无线网络。

无线自组网络采用不需要基站的“对等结构”移动通信模式，该网络中没有固定的路由器，它的所有用户都可以移动，并且支持动态配置和动态流量控制；每个系统都具备动态搜索、定位和恢复连接的能力。这些行为特征可以用“移动分布式多跳无线网络”或“移动的网络”来描述。例如，员工每人有一台带有天线的便携式计算机，他们被召集在一间房间里开会，计算机可以连接到一个暂时的网络，会议完毕后网络将不再存在。

（2）无线局域网协议

无线局域网标准 802.11 定义使用红外、跳频扩频与直接序列扩频技术，数据传输速率为 1Mbps 或 2Mbps 的无线局域网标准。该协议使用跳频扩频技术，传输速率为 1Mbps、2Mbps、5.5Mbps 与 11Mbps 的无线局域网标准。该协议将传输速率提高到 54Mbps。无线局域网是当前网络研究的一个热点问题，当前 802.11 标准已从 802.11b、802.11a 发展为 802.11j，对多种频段无线传输技术的物理层、MAC 层、无线网桥，以及 QoS 管理、安全与身份认证做出一系列的规定。致力于 WLAN 技术推广的 Wi-Fi 联盟是由业界成员参加，它的作用是促进 802.11 无线局域网标准的推广与应用。

（3）无线城域网与 IEEE802.16 标准

宽带无线接入 802.11 标准无线局域网作为局域网接入方式的一种补充，已在个人计算机无线接入中发挥重要作用。在无线通信技术应用广泛的背景下，如何在城域网中应用无

线通信技术的课题就被提出。对于城市区域的一些大楼、分散的社区，架设电缆与铺设光纤的费用往往要大于架设无线通信设备，人们开始研究在市区范围的高楼之间利用无线通信手段解决局域网、固定或移动的个人用户计算机接入互联网的问题。

尽管 802.11 与 IEEE 802.16 标准都针对无线环境，但是由于两者的应用对象不同，因此在采用的技术与协议解决问题的重点也不同。802.11 标准的重点在于解决局域网范围的移动结点通信问题，而 IEEE 802.16 标准的重点是解决城市范围内建筑物之间的数据通信问题。IEEE 802.16 标准的主要目标是制定工作在 2～66GHz 频段的无线接入系统的物理层与介质访问控制层规范。IEEE 802.16 是一个点对多点的视距条件下的标准，用于大数据量的传输。IEEE 802.16a 增加非视距和对无线网状网结构的支持。IEEE 802.16 与 IEEE 802.16a 经过修订后，被统一命名为 IEEE 802.16d。按 IEEE 802.16 标准建立的无线网络覆盖一个城市的部分区域，同时由于建筑物位置是固定的，它需要在每个建筑物上建立基站，基站之间采用全双工、宽带通信方式工作。IEEE 802.16 标准提供两个物理层标准 IEEE 802.16d 与 IEEE 802.16e。IEEE 802.16d 主要针对固定的无线网络部署，IEEE 802.16e 针对火车、汽车等移动物体的无线通信标准问题。与 IEEE 802.16 标准工作组对应的论坛组织为 WiMAX，与致力于 WLAN 推广应用的 Wi-Fi 联盟很类似，它是由业界成员参加的，致力于 IEEE 802.16 标准的推广与应用。无线接入技术以投资少、建网周期短、提供业务快等优势，已经引起产业界的高度重视。

（4）蓝牙、无线个人区域网与 ZigBee

1）蓝牙技术。Ericsson 公司对于如何在无电缆的情况下，将移动电话和其他设备（如 PDA）连接起来产生浓厚的兴趣。Ericsson 公司与 IBM、Intel、Nokia 和 Toshiba 等公司发起一个项目，开发了用于将计算机与通信设备、附加部件和外部设备，通过短距离的、低功耗的、低成本的无线信道连接的无线标准。这个项目被命名为蓝牙（Bluetooth）。它与一位丹麦国王的名字有关，即公元 940—985 年间的丹麦国王 Harald Blatand。据说在他统治期间统一了丹麦和挪威，因此就将“Blatand”近似翻译成“Bluetooth”，中文直译为“蓝牙”。由于这项技术是在斯堪的纳维亚地区产生，因此技术的创始人就用这样的名字命名，以表达他们要像当年的丹麦国王统一多国一样，统一世界很多公司“短距离无线通信”技术和产品的初衷。

蓝牙无线通信技术是作为一个技术规范出现，该规范是蓝牙特别兴趣小组 SIG 中很多公司合作的结果。目前，SIG 共有 1800 多个成员，包括消费类电子产品制造商、芯片制造厂家与电信业等。SIG 的主要任务是致力于发展蓝牙规范，但是它也许不会发展成一个正式的标准化组织。

蓝牙技术的特点：无线通信产品要能方便、快速地普及，通信频率在全球各国统一开放的频段上，该频段的产品无须事先申请和缴纳频率使用费。蓝牙技术符合这个条件，它

的工作频率在国际开放的 ISM 2.4GHz 上。为了避免相同频率电子设备之间的干扰，蓝牙技术还采用了调频扩展技术。

蓝牙技术在协议设计之初就确定了芯片轻、薄、小的特点。以典型的爱立信的蓝牙芯片为例，体积只有 10.2mm×14mm×16mm，发射功率控制在 1mW，作用距离可以达到 10m，芯片价格控制在 5 美元以内，可以嵌入在各种设备之中。

蓝牙技术的应用：蓝牙技术有十分突出的特点，它可以应用于几乎所有的电子设备，例如移动电话、蓝牙耳机、便携式计算机的鼠标、打印机、投影仪、数字相机、门禁系统、遥控开关、各种家用电器等。蓝牙技术支持点—多点通信。利用蓝牙技术可以在 10m 范围内实现 7 个活动蓝牙设备，以及最多 255 个处于待机蓝牙设备组成一个无线个人区域网络。

蓝牙规范与 IEEE 802.15 标准：虽然蓝牙技术最初的目标只是解决近距离数字设备之间的无线连接，但是很快扩大到无线局域网的工作领域中。尽管这样的转变使该标准更有应用价值，但也造成它与 IEEE 802.11 标准竞争的局面。在蓝牙规范 1.0 版发表后不久，IEEE 802.15 标准组织决定采纳蓝牙规范作为基础，并开始对它进行修订。从网络体系结构来看，它覆盖从物理层到应用层的全部内容。IEEE 802.15 标准组仅对物理层和数据链路层进行标准化，蓝牙规范的其他部分并没有被纳入该标准。IEEE 标准来管理这样开放的标准，有助于这项技术的推广和应用，但是如果在一项事实上的工业标准出现后，又出现一个与它不兼容的新规范，对于技术发展来说也是很麻烦的。

2）无线个人区域网与协议。随着手机、便携式计算机和移动办公设备的广泛应用，人们逐渐提出自身附近几米范围内的个人操作空间设备联网的需求。个人区域网络与无线个人区域网络在这个背景下出现。

IEEE 802.15 标准组织致力于个人区域网的标准化工作，它的任务组 TG4 制定 IEEE 802.15.4 标准，主要考虑低速无线个人区域网络（Low-Rate WPAN，LR-WPAN）应用问题。2003 年，IEEE 批准了 LR-WPAN 标准——IEEE 802.15.4。它为近距离范围内不同设备之间低速互联提供统一标准。与 WLAN 相比，LR-WPAN 只需很少的基础设施，甚至不需要基础设施。LR-WPAN 的特征与无线传感器网络有很多相似之处，很多研究机构也将它作为无线传感器网络的通信标准。

3）ZigBee 的特点。ZigBee 是一种面向自动控制的低速、低功耗、低价格的无线网络技术。ZigBee 的通信速率要求低于蓝牙，但要求由电池供电，在不更换电池情况下工作几个月，甚至几年。同时，ZigBee 网络的结点数量、覆盖规模比由蓝牙技术支持的网络大得多。ZigBee 无线设备工作在公共频道，在 2.4GHz 时传输速率为 250Kbps，在 915Mbps 时传输速率为 40Kbps。ZigBee 的传输距离为 10～75m。ZigBee 适应于数据采集与控制的点多、数据传输量不大、覆盖面广、造价低的应用领域，在家庭网络、安全监控、医疗保健、工业控制、无线定位等方面展现了重要的应用前景。

ZigBee 技术的特点主要表现在：

- ZigBee 网络结点工作周期短、收发数据量小，不传输数据时处于“睡眠状态”。传输数据时由担任“协调器”的结点唤醒。采取这种工作模式的优点是节省电能，延长网络工作时间。
- ZigBee 采用碰撞避免机制并为需要固定带宽的通信业务预留专用时间片，以避免发送数据的冲突。由于在 MAC 层采用确认机制，以保证结点之间通信的可靠性。
- ZigBee 协议结构简单，实现协议的专用芯片价格低廉，系统软件结构力求简单，从而降低了系统的造价。通信模块芯片价格预期可以降到 1.5～2.5 美元。
- ZigBee 标准与蓝牙标准的延时参数相比，ZigBee 结点的休眠/工作状态转换需要 15ms，入网时间需要 30ms，而蓝牙结点的入网时间需要 3～10s。
- 1 个 ZigBee 网络最多容纳 1 个主结点和 254 个从结点，1 个区域中可以有 100 个 ZigBee。
- ZigBee 提供了数据完整性检查与加密算法，以保障网络的安全。

基于 ZigBee 技术的无线传感器网络已成为产业界十分关注的一个研究方向。

3.2 网络频率分配

在无线通信中，频率资源非常有限，人们的需求却越来越多。如何有效地分配频率是运营商亟待解决的一个非常重要和困难的问题。信道分配问题（Channel Assignment Problem，CAP）是频率分配问题的理论模型，最早在 20 世纪 60 年代提出。近年来，由于无线电话网络，卫星通信、广播电视和军事通信等领域的迅速发展，频率资源变得越来越紧张，如何节省并有效地利用频率已成为移动无线领域中的一个核心问题，其中频谱资源复用可以解决这个问题。

3.2.1 频率分配的核心内容

（1）基本概念

频率分配是在满足各种约束的条件下，将可用频点分给小区，这样使得网络中的小区间干扰尽可能小。为满足最大可能的需求，同时避免不可接收的干扰电平，频谱要求载频用最有效的方式在空间复用。六边形蜂窝网络理论已被用于蜂窝无线通信系统的频率分配问题。这一理论也有几个变体，其中非常重要的是蜂窝扇形化和复用分割。但后来的研究指出，六边形理论不能给实际频率分配问题提供适当的解决方案，主要原因为：

- 因地理条件限制，实际基站是不规则的网络。

- 传播条件通常是非常不规则的，所以干扰电平不仅取决于距离。
- 话务密度空间变化导致不同的蜂窝信道需求变化。
- 环境限制某些频率的使用。

“信道分配”有着多种定义形式，但其核心内容都是一致的，即在采用信道复用技术的小区制蜂窝移动系统中，在多信道共用的情况下，以最有效的频谱利用方式，为每个小区的通信设备提供尽可能多的可用信道。

在蜂窝移动通信系统中，对于不同的多址系统，信道可能有不同的含义。对于频分多址（FDMA）系统，信道分配是指频率（或频点）分配；对于时分多址（TDMA）系统，一个频率被划分成多个时隙，一个时隙即为一个信道，信道分配是指时隙的分配；对于码分多址（CDMA）系统，信道分配是指地址码的分配。而在本小节中讨论的信道分配是指频率分配，又称为频点分配。

（2）频率分配技术

由于频率资源有限，对小区频率分配时，需要使用频率复用技术。在蜂窝网络中，根据无线电传输路径损耗特性，一个基站使用的频率可以在距离该基站很远距离的另一个基站重复使用。每个基站覆盖的范围成为一个小区，使用相同频率的小区称为同频区。为避免同频干扰不会影响通信质量，同频小区必须有足够远的距离。频率复用技术包括普通频率复用、MRP（Multiple ReusePattern）、同心圆复用等。

（3）频率分配策略

移动通信系统采用蜂窝结构有效地增加了系统的用户数量，但由于有限的频率资源，存在一个信道分配策略（Channel Assignment Strategy，CAS）问题。最优信道分配方案可以提高系统的服务质量，降低运营商的基础设施投资。根据不同的特点和应用，把 CAS 进行不同的分类。最常见的是根据信道与小区的关系，可以把 CAS 分为固定信道分配（FCA）策略、动态信道分配（DCA）策略和混合信道分配策略（HCA）。根据具体实施模式，CAS 还可分为集中式和分布式两种。

1）固定信道分配策略（FCA）。FCA 是把一个单信道固定分配给多个用户，如果在一个特定的用户组同时有两个或两个以上的用户发起呼叫，这时一个信道在同一时刻只能有一个用户占用，其他用户只能等待信道。

当部署一个新的系统，并且预期负荷均匀分布时，FCA 战略是一个很好的选择，它在繁重荷载下也完成得很好。但当移动通信系统中的负荷量分配随空间和时间更频繁的变化，或非均匀时，这种均匀分布的信道在高负荷量的小区可能导致阻塞率高，而在低负荷量的小区出现空闲信道。这是 FCA 的一个主要缺点。因此，对这样的系统需要利用 FCA 策略进行非均匀信道分配，分配给每个小区的信道数应由该小区实际需要承担的负荷量决定。因此，高负荷量的小区比低负荷量的小区可以分配到更多的信道，从而提高了信道的有效

利用率。然而，当负荷量随时间变化较大时，还是没有足够的信道可以利用。由于简单的FCA 策略不能重新分配渠道，在不断变化的负荷量条件下不能灵活处理和邻近小区的共享频谱资源问题，从而导致信道的利用率很低。但 FCA 策略简单易行，能实现快速分配。克服负荷量非均匀分布影响的另一种方法是从邻近小区借用空闲信道。信道借用策略是，当一个地区没有空闲信道，如果满足干扰约束条件，就可以从邻近小区借用一个信道接收新的呼叫。信道借用只能在对相邻小区产生的影响最小的情况下使用。在低话务负荷量和中话务负荷量条件下，信道借用方案更好，但在高负荷量条件下，FCA 优于信道借用。

2）动态信道分配策略 DCA。为了改善 FCA 策略信道利用率低的缺点，人们又开始研究了动态信道分配策略。DCA 通过采用动态方式分配信道，克服了 FCA 策略对话务量的时间和空间变化缺乏自适应的缺点。在 DCA 中，信道和小区没有固定的联系，只要同频信道复用距离和干扰约束条件得到满足，每个信道都能在任何小区中使用，并且只在通话期间小区才拥有信道，所有信道都被放在一个中央信道池中，并且随着系统中呼叫的到达，中央信道池负责搜寻具有对系统费用最小的信道分配给小区。一旦呼叫结束，信道就返回给中央信道池。

DCA 对空间和时间上不同的话务条件可以自动地适应，在分配过程中为了确定在特定情况中是否可以利用某些信道，不需要关于信道状况的信息。DCA 算法不需要信道规划，在低、中等话务负荷条件下比 FCA 策略有更好的性能。但是，当系统出现高话务量时，DCA 策略并不优于 FCA 策略，尤其当话务量分布是非均匀时。这主要是因为 DCA 策略中分配信道的任意性，只要同一信道集的小区按平均相隔的距离大于最小同频复用距离即可。DCA 策略的主要缺点是每一个基站的收发信机除了必须能在标称信道上工作外，而且有些情况应能在全部信道上工作，增加了投资费用。

3）混合信道分配 HCA。HCA 策略是一种将 FCA 和 DCA 混合使用的分配技术。在 HCA 中把用来服务的所有可利用信道分成两个子集。一个信道子集根据 FCA 策略分配给系统中的小区。另一个信道子集保存在一个信道中央池中，根据需求动态地分配给小区以增加灵活性。不管在什么情况下，第一个子集的信道只能在所分配的小区使用，而第二个子集中的信道可以分配给系统所有的小区使用。DCA 在低话务量情况下具有最佳性能。当话务量不断增加时，固定分配因其对信道的最佳复用，其性能变得更好。HCA 在系统处于基本话务量时作用如同在低话务量条件下的 DCA。这是因为话务量是由固定信道组和动态信道组共同承载，而不是平分，因此在低话务量条件下承载量增加时阻塞率并不大。然而当承载的话务量高于基本话务量一定程度时，具有较多动态信道的 HCA 的呼叫阻塞率开始不断增大。这种现象也是 DCA 策略的一个特点。HCA 策略在非均匀话务量条件下将显示它的优越性，因为其中的动态信道组能够使系统更加灵活，克服话务量的随机波动。

3.2.2　频率分配的数学模型

蜂窝通信的关键是频率复用，即在一个小区内使用的信道可以在其他小区重复使用。但是，复用就容易引起干扰问题。所谓信道分配问题就是要尽量降低这种干扰，从而改善整个网络。信道分配必须满足以下三种约束。

1）同信道约束（CCC）：是指使用相同信道小区的空间间隔要求，满足该条件的两个小区可以分配相同的信道。同一个信道不能在其同频干扰范围内再次使用。

2）邻信道约束（ACC）：是指相邻小区的信道间隔要求。不能同时把相邻信道分配给相邻小区使用。

3）同小区约束（CSC）：同一个小区内的所有信道之间必须要有一定的频率间隔，通常要大于 ACC 所要求的。

下面介绍一下信道分配问题（CAP）的数学模型。首先我们将所有的信道（频点）用 l，2，3，…等正整数依次标号。假设一个由 n 个小区组成的蜂窝系统，考虑前面提到的三种信道干扰约束，我们可以定义一个 $n\times n$ 维对称矩阵，称之为约束矩阵 $\boldsymbol{C}$（或称为兼容矩阵、干扰矩阵），式（3-1）是约束矩阵的数学表达式。约束矩阵 $\boldsymbol{C}$ 中的非对角元素 $c_{ij}(i\neq j)$ 表示分配给第 i 小区的频点与第 j 小区中的频点之间最小间隔，而矩阵 $\boldsymbol{C}$ 中的对角线元素 c_{ii} 表示分配给第 i 小区的一组频点之间的最小频点间隔。因此我们知道 CCC 可以用 $c_{ij}=1$ 来表示，而 ACC 和 CSC 可以分别定义 $c_{ij}\geqslant 2$ 和 $c_{ij}\geqslant 1$ 来表示，$c_{ij}=0$ 表示小区可以使用相同的信道（频点）。

$$\boldsymbol{C}=[c_{ij}]\quad i,j\leqslant n \tag{3-1}$$

通过对系统中每个小区的话务量分析（根据人口指数和用户总数、忙时发生的平均话务量和服务等级），我们可以定义一个 n 维的矢量 $\boldsymbol{D}$（称为需求向量）来表示每个小区的频点需求。需求向量 $\boldsymbol{D}$ 中的第 i 个元素 d_i 表示第 i 个小区需要的频点数。令 f_{ik} 为分配给第 i 个小区的第 k 个频点，其中 $i=1,\cdots,n$；$k=1,\cdots,d_i$。这样系统所需总频点数可以表示为

$$M=\max\{f_{ik}\}\qquad i=1,\cdots,n;\ \ k=1,\cdots,d_i \tag{3-2}$$

若已知约束矩阵 $\boldsymbol{C}$ 和需求向量 $\boldsymbol{D}$，CAP 的主要目的就是希望找到这样一种 CAS $\{f_{ik}\}$（Channel Assignment Strategy，CAS，信道分配策略），它具有最少的频点数 M，并且服从下列频点间隔约束：

$$|f_{ik}-f_{j1}|\geqslant c_{ij} \tag{3-3}$$

$i,j=1,\cdots,n$；$k=1,\cdots,d_i$；$l=1,\cdots,d_j$，$(i,k)\neq(j,l)$

传统的图论方法将 CAP 构成为“最小集合”问题，可以作为一个组合优化问题表示为

$$\min M=\max_{i,k}\{f_{ik}\} \tag{3-4}$$

条件：$|f_{ik}-f_{j1}|\geqslant c_{ij}$

其中：$1\leqslant i\leqslant n$，$1\leqslant j\leqslant n$，$1\leqslant k\leqslant d_i$，$1\leqslant l\leqslant d_j$，$(i,\ k)\neq(j,\ l)$

3.3 网络中的信道分配

信道是无线通信的发送端和接收端之间的通道，无线电波从发射端传输到接收端不存在一个物理连接，其传播路径也可能不止一个，为了形象地描述发送端和接收端之间的工作，我们设想信道是连接两者之间的一个不可见的通道。信道有频率带宽。

无线信道中电波传播路径不是单一的，而是多路径多反射波的合成。当波通过不同的路径时，每个路径距离是不同的，每个路径来的反射波到达时间也是不同的，形成了各个信号不同的延迟。当发送者发送一个很窄的脉冲信号，移动台接收的信号来自许多不同的时间延迟脉冲信号，我们称为时延扩散。

不同路径的反射波到达的时间不同，其相位也不同。不同相位的信号在接收端产生叠加，有时加强（同一方向），有时减弱（相反的方向）。因此，接收信号的幅度将大大改变，从而产生了快衰落。这一衰落的原因是多路径造成的，因此它被称为多径衰落。

此外，接收到的信号除了瞬时值快衰落以外，平均值也会出现缓慢的变化。主要由区域位置的变化和气象条件变化引起的，折射波随着时间而变化，多径传播在固定点信号延迟随之发生变化。这种由阴影效应和气象因素引起的信号变化，称为慢衰落。

此外，由于移动通信移动台的移动性，无线信道将产生多普勒效应。在移动通信中，当移动台向基站移动时，频率变高，远离基站时，频率变低。我们在移动通信中要充分考虑多普勒效应。虽然在日常生活中移动速度受到限制，不可能带来很大的频率偏移，但不可否认地会给移动通信带来影响，增加了移动通信的复杂性。

综上所述，无线信道包括无线多径传播、传播延迟、衰落特性以及多普勒效应。在移动通信领域，我们应充分考虑这些特点并研究解决方案。

进行无线网络安装，一般使用无线网络设备自带的管理工具，设置连接参数，无论哪种无线网络的最主要的设置项目都包括网络模式（集中式还是对等式无线网络）、SSID、信道、传输速率四项，只不过一些无线设备的驱动或设置软件将这些步骤简化了，一般使用默认设置（也就是不需要任何设置）就能很容易地使用无线网络。但很多问题是因为追求便利而产生的。我们知道，常用的 IEEE 802.11b/g 工作在 2.4～2.4835GHz 频段，这些频段被分为 11 或 13 个信道。当在无线 AP 无线信号覆盖范围内有两个以上的 AP 时，需要为每个 AP 设定不同的频段，以免共用无线信道发生冲突。而很多用户使用的无线设备的默认设置都是信道为 1，当两个以上的这样的无线 AP 设备相遇时冲突就在所难免。

众所周知，目前主流的无线标准都是由 IEEE（美国电气电工协会）所制定的，在 IEEE 认定的三种无线标准 IEEE 802.11b、IEEE 802.11g、IEEE 802.11a 中，其信道数是有差别的。

（1）IEEE 802.11b

采用 2.4GHz 频带，调制方法采用补偿码键控（CKK），共有“3”条不重叠的传输信道。传输速率能够从 11Mbps 自动降到 5.5Mbps，或者根据直接序列扩频技术调整到 2Mbps 和 1Mbps，以保证设备正常运行与稳定。

（2）IEEE 802.11a

扩充了标准的物理层，规定该层使用 5GHz 的频带。该标准采用 OFDM 调制技术，共有“12”条非重叠的传输信道，传输速率范围为 6～54Mbps。不过此标准与 IEEE 802.11b 标准并不兼容。支持该协议的无线 AP 及无线网卡，在市场上较少见。

（3）IEEE 802.11g

该标准共有“3”条不重叠的传输信道。虽然同样运行于 2.4GHz，但向下兼容 IEEE 802.11b，而由于使用了与 IEEE 802.11a 标准相同的调制方式 OFDM（正交频分），因而能使无线局域网达到 54Mbps 的数据传输率。

在 802.11b/g 情况下，可用信道在频率上都会重叠交错，导致网络覆盖的服务区只有 3 条非重叠的信道可以使用，结果这个服务区的用户只能共享这 3 条信道的数据带宽。这 3 条信道还会受到其他无线电信号源的干扰，因为 802.11b/g WLAN 标准采用了最常用的 2.4GHz 无线电频段。而这个频段还被用于其他方面，如蓝牙无线连接、手机甚至微波炉，这些应用在这个频段产生的干扰可能会进一步限制 WLAN 用户的可用带宽。

而在同样是 54Mbps 的传输速率的 802.11g 与 802.11a 标准中，802.11a 在信道可用性方面更具优势。这是因为 802.11a 工作在更加宽松的 5GHz 频段，拥有 12 条非重叠信道，而 802.11b/g 只有 11 条，并且只有 3 条是非重叠信道（Channel 1、Channel 6、Channel 11 或 Channel 13）。所以 802.11g 在协调邻近接入点的特性上不如 802.11a。由于 802.11a 的 12 条非重叠信道能给接入点提供更多的选择，因此它能有效降低各信道之间的冲突。

3.4　结点的功率与功耗分配

3.4.1　功率分配的作用

对于不同的通信系统，因为其应用目的不同，功率控制技术所起的作用也是不一样的。在最早的无线分组网络中，结点通常是使用专用线路供电，也没有能量受限的问题，因此，如何提高无线分组的网络容量，减少每个结点之间的干扰是需要考虑的主要问题，功率控

制主要是用来调整传输距离。蜂窝移动通信系统和无线分组网络有着明显的不同，各种蜂窝移动通信系统有一个固定的基站，基站的处理能力大大高于系统中移动结点的处理能力，并有足够的能源供应，而移动结点由电池供电，处理能力弱，基地站和移动结点之间的不对称是蜂窝移动通信系统中的一个重要特征。随着用户数量的增多，如何降低用户间的干扰，提高网络容量，成为系统功率控制的主要目标。无线传感器网络的功率控制是在不降低系统性能的前提下，尽可能地降低结点的发射功率，从而降低结点的能量消耗，提高网络的生存时间和系统能量效率。有效功率控制策略能减少网络中结点不必要的能量消耗，延长网络的生命周期。

3.4.2 功率分配对系统的影响

功率控制对于无线传感器网络的性能影响显著，主要表现在以下几方面。

（1）功率控制对网络能量有效性的影响

功率控制对网络能量效率的影响包括降低结点发射功率和降低网络总能耗。在结点的分组传输过程中，功率控制可通过信道估计或反馈控制信息，在确保信道连通的条件下减少发射功率的富余量，从而减少发送端结点能耗。随着源结点发射功率减小，它可以影响邻居结点数目使之减少，从而节省了网络中其他不相关结点的接收能量消耗，因此而降低整个网络的能耗。

（2）功率控制对网络连通性和拓扑结构的影响

网络连接性和拓扑结构都与发射功率的大小有关。结点的发射功率太低，会使部分结点无法建立通信连接，造成网络隔离；结点发射功率过大，可以保证网络连通性，但会导致网络增加竞争强度，从而使网络不仅在结点的发射功率消耗太多能量，也会因为高强度的竞争导致数据包丢失或重传，从而使网络整体能耗增加和性能下降。网络中的结点通过功率控制和骨干网络结点的选择，消除不必要的通信结点之间的联系，形成一个优化的数据转发网络结构，或在满足网络连通性的前提下，选择结点最优的单跳可达邻居数。通过功率控制技术来控制网络的拓扑特性，主要是通过寻求最优发射功率和相应的控制策略，在保证网络连通性的同时优化拓扑结构，以满足网络应用性能要求。

（3）功率控制对网络平均竞争强度的影响

结点的发射功率影响网络的平均竞争强度。设网络中结点密度为ρ，发射半径为 r，则发射结点范围内的邻居结点数量为 ρr^2，由于任意一个结点通过的流量与 $1/r$ 成正比，因此可得网络的平均竞争强度与结点的发射半径 r 成正比。功率控制则可通过降低网络中结点的发射功率减小网络中的冲突域，降低网络的平均竞争强度。

（4）功率控制对网络容量的影响

功率控制对于网络容量的影响一方面表现在可有效减少数据传输结点所能影响的邻居

结点的数量，允许网络内进行更多的并发数据传输；另一方面，由于结点通信的传输范围越大，网络中的冲突就会越多，结点通信更容易发生数据包丢失或重传，通过功率控制技术可有效减小网络中的冲突域，从而降低通信冲突的概率。功率控制在这两方面的作用均有助于网络容量的提升。

（5）功率控制对网络实时性的影响

无线自组织网络采用多跳路由的方式对消息进行传递，分组的每一跳均会经历处理延时、传播延时和队列延时三个阶段。处理延时 T_{proc} 包括接收机接收分组、解码以及重传分组所需要的时间，传播延时 T_{prop} 是分组在介质中传播所消耗的时间，队列延时 T_{queu} 则是分组由于在队列中排队等待所造成的延时。设网络中分组传递所需的路由跳数为 N，则端到端（end to end）的分组延时如下。

$$T_{\text{end}}=（T_{\text{proc}}+T_{\text{prop}}+T_{\text{queu}}）\times N \tag{3-5}$$

在网络中较低的发射功率需要较多的路由跳数才能到达目的结点，而较高的发射功率则可有效减少源结点与目的结点之间分组传递所需的跳数。分组的处理延时正比于路由的跳数，队列延时反比于网络的竞争强度，而传播延时受网络状态的影响较小。由此可见，高发射功率会导致较长的队列延时，而低发射功率则会增长分组的处理延时。基于上述分析，功率控制可根据网络状态，策略性的改变结点的发射距离，从而使网络具有较好的实时性能。

功率控制技术可运用于多种通信网络中（如蜂窝移动通信网络、WLAN、MANET、传感器网络等），但由于系统的应用目的不同，功率控制所起的作用也不尽相同。Ad Hoc 网络的研究工作起步相对较早，研究者们对于功率控制在 Ad Hoc 网络中的应用已经开展了大量的研究工作，并取得了许多阶段性的研究成果。Ad Hoc 网络是一种面向服务的网络。因此，功率控制在 Ad Hoc 网络中的应用主要以提高系统容量，为用户提供数据分组传输的服务质量保证为目的和设计原则。

传感器网络在某种程度上可以被视为一种特殊的 Ad Hoc 网络，功率控制同样可被引入到传感器网络中以改善网络的性能。然而，两者之间虽然存在着一些相似之处，但也同时存在着很大的差别：传感器网络是集成了监测、控制以及无线通信的资源受限型网络系统，传感器结点具有的能量、处理能力、存储能力和通信能力等都十分有限，能源的高效使用是系统设计的首要目标。资源受限、大规模使用、网络动态性强等传感器网络所具有的系统特性和现实约束使得一些为 Ad Hoc 网络设计的功率控制协议和算法并不能直接适用。但是，由于功率控制对于无线自组织网络多个方面的性能均具有显著影响，因此国内外不少研究已经将功率控制引入到传感器网络的协议设计中。

传感器网络研究领域中出现的新特点和新方向，使以往主要针对网络能量有效性的研究方法存在着较大的局限性，如果仅满足网络的能耗需求，而不能保证系统运行的其他性能，整个网络将不具有任何实用价值。在现阶段的研究过程中，应从系统的实用性要求出

发，对传感器网络应用进行分类，并针对不同应用类别的特点设计和优化网络实现机制。基于上述分析可以得出传感器网络功率控制技术的设计目的和原则，即针对具体应用分类，通过策略性的改变结点的发射功率，在保证系统性能要求的前提下，尽可能地降低网络的通信能耗，提高能量效率，延长系统的生存时间。

3.4.3 典型的功率控制协议与算法

由于单一的协议无法满足系统各种应用的需求，人们研究了众多的功率控制协议。功率控制算法是一个典型的网络控制论问题，故可按照以下方法进行分类。

1）开环控制、闭环控制和开环闭环混合控制。开环功率控制是指网络中的结点以反比于接收到的平均功率水平的参数量调整发射功率值；闭环功率控制是指发送结点根据接收结点的反馈控制信息动态地改变发射功率；开环闭环混合功率控制则是将两种控制机制结合应用于网络中。

2）集中控制和分布式控制。在集中功率控制机制中，存在一个管理中心集中调整网络中结点的发射功率水平；而在分布式功率控制中则不存在具有集中控制能力的管理中心，每个结点根据局部信息调整自身的发射功率值。

3）基于 RSSI 指标、基于 SIR 指标和基于 BER 指标。功率控制可分别以接收信号强度 RSSI、信号干扰比 SIR 或误码率 BER 为指标，控制调整网络中结点的发射功率值。

4）定步长控制和自适应步长控制。定步长功率控制是指结点策略性地以确定的调整步长量控制发射功率值；而自适应步长功率控制则是指结点根据信道变化的估计量自适应地调整结点的发射功率。

5）连续控制和离散控制。功率控制过程可以是连续量，也可以是离散量，因此可分为连续功率控制和离散功率控制。

6）单信道控制和多信道控制。单信道功率控制是指网络使用单一共享信道，多信道功率控制则是指采用多个信道完成网络控制和消息传递。

7）统一控制和独立控制。统一功率控制是指网络中结点的发射功率可调整，但所有结点均采用同一发射功率值；独立功率控制是指每一个结点均可独立调整自身的发射功率值，网络中结点之间的发射功率水平不尽相同。

8）网络级控制、邻居结点级控制和独立结点级控制。分类方法 8）是对方法 7）的进一步细化，它基于分组级分析方法，从网络本身问题的角度出发对功率控制算法进行分类。网络级功率控制是指网络所有结点均使用统一的功率控制值发送分组；邻居结点级功率控制是指每个发送结点均使用可覆盖所有邻居结点的功率值发送分组，结点之间的发射功率值并不相同；独立结点级功率控制则是指发送结点可以针对每个单一的目的结点自适应的调整发射功率水平。

3.5 接口技术与标准

3.5.1 SCSI 小型计算机系统接口

SCSI（Small Computer System Interface）是一种专门为小型计算机系统设计的存储单元接口模式，可以对计算机中的多个设备进行动态分工操作，对于系统同时要求的多个任务可以灵活机动的适当分配。

（1）SCSI 连接器的类型

SCSI 连接器分为内置和外置两种。内置数据线的外型和 IDE 数据线一样，只是针数和规格略有不同，主要用于连接光驱和硬盘，40 针 IDE 线有 40 根导线，40 针 ATA66 有 80 根导线，SCSI 内置则分为 50 针、68 针和 80 针。至于 SCSI 外置数据线，就有以下几种规格，它们的密度均不相同。

Apple SCSI 共有 25 针，分为两排，8 位，如图 3-3 所示，常用于 Mac 机和旧式 Sun 工作站。

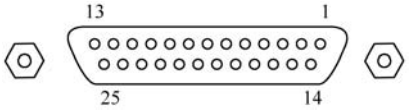


图 3-3　Apple SCSI 数据线

Sun Microsystem 的 DD-50SA 共有 50 针，分为三排，如图 3-4 所示。

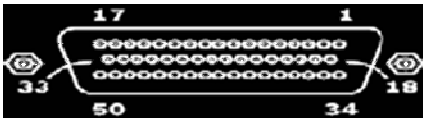


图 3-4　DD-50SA 数据线

SCSI-2 共有 50 针，分为两排，8 位，如图 3-5 所示。

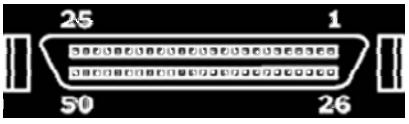


图 3-5　SCSI-2 数据线

Centronics 共有 50 针，分为两排，8 位，有点像并行口，它可以连接的设备数目最多，

如图 3-6 所示。

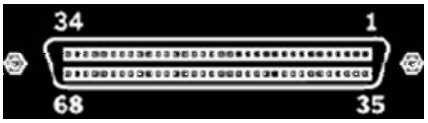


图 3-6　Centronics 数据线

SCA 共有 80 针，分为两排，如图 3-7 所示。



图 3-7　SCA 数据线

SCSI-3 和 Wide SCSI-2 共有 68 针，分为两排，16 位，如图 3-8 所示。旧式 DEC 单终结 SCSI 使用 68 针高密接口。

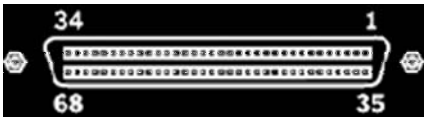


图 3-8　SCSI-3 和 Wide SCSI-2 数据线

（2）SCSI 的有关规定

SCSI 1 是 1986 年的原始规定，第一个 SCSI 标准，最多允许连接 7 件设备，最大传输速度为 5Mbps。

SCSI 2 又称为 Fast SCSI（快速 SCSI），在 SCSI 1 的基础上做了诸多改善，但是直到 1994 年之前没有普遍应用。SCSI 2 精简了一些选项，增加了可靠性，把传输速度提高到 10Mbps。

Fast Wide SCSI 是 SCSI 2 的一种类型，总线宽度增加一倍，成为 16bit 总线，传输速度提高到 20Mbps，一个控制器可以连接 14 件设备。

Ultra SCSI 也是 SCSI 2 的一种类型，使用原始的 8-bit 总线，但是最高传输速度为 20Mbps，单个控制器可以连接的设备仍是 7 件。

Ultra Wide SCSI 又称作 Wide Ultra SCSI，如同 Fast Wide SCSI 一样使用 16bit 总线，最高传输速度为 40Mbps，一个控制器可以连接 14 件设备。

Ultra 2 SCSI 使用 8bit 总线，但内部时钟速度加倍，最高传输速度达到 40Mbps，单个控制器可以连接的设备仍是 7 件。

Wide Ultra 2 SCSI 在一段时间内是最快的 SCSI，使用 16bit 总线，最高传输速度为 80Mbps，内部时钟速度加倍，一个控制器可以连接 7 件设备。

Ultra 3 SCSI 又称为 SCSI 160，是极快的 SCSI 标准。使用 32bit PCI 槽的控制器最高传输速度为 80Mbps，使用 64bit PCI 槽的控制器最高传输速度为 160Mbps，一个控制器可以连接 14 件设备。SCSI 3 已经慢慢地降低了价格，它将是 24bit/96kHz 录音硬盘的最佳选择。

Ultra SCSI 320 是新的 SCSI 标准，刚刚开始应用。Ultra SCSI 320 使用 32bit PCI 槽允许最高传输速度为 160Mbps，使用 64bit PCI 槽的控制器最高传输速度为 320Mbps。SCSI 320 使用 16bit 总线，兼容 SCSI 160。

（3）SCSI ID 和总线终结器

许多 SCSI 用户都有这样的经历，在插上插头后，操作系统不承认，检查后才发现终结器和 ID 没有设置好。ID（identify）作为 SCSI 设备在 SCSI 总线的一个独特的标识符，绝对不允许重复，可选的范围从 0～15，SCSI 主控制器通常占 ID7，也就是说我们可以用在设备上的编号共有 15 个。总线终结器可以告诉 SCSI 主控制器总线在哪里结束，并发送一个反射信号给控制器必须有反应，必须在两个物理终端做一个结束信号才能使用 SCSI 总线。一个常见的错误是把终结设定在 ID 最高或最低的地方，而不是设置在物理终端的 SCSI 设备上。事实上，SCSI 设备始终处于链型连接状态，按顺序就可以说出哪一个是终结设备。终结方式有三个：自终结设备、物理总线终结器和自终结电缆。大多数新的 SCSI 设备有自终结跳线，只要非终结设备的自终结跳线设置成 OFF 就可以避免冲突；物理总线终结器是一种接头，并分为主动和被动型，主动型利用电压调节器操作，被动型使用总线信号上的能源信号操作，比起主动型，被动型更准确；自终结电缆可以用来代替物理总线终结器，也是一种硬件，非常昂贵，常用于两主机连接同一个物理设备，如双服务器访问同一个物理 SCSI 硬盘。通过检查 SCSI ID 和总线终结器，我们可以找到办法解决大多数冲突，这是 SCSI 设备的用户必须的注意一点。

（4）IDE 和 SCSI 的比较

我们从性能、价格、易用性、扩展性多方面因素来对二者进行比较。

从性能上说，SCSI 要比 IDE 好。SCSI 控制器上有一个相当于 CPU 的芯片，能够处理大部分工作，减轻了中央处理器的负担（CPU 占用率）。SCSI 设备的转速、缓存容量和数据传输率均比 IDE 高，同时 SCSI 的速度要比 IDE 的速度快。

价格方面，SCSI 的价格比较昂贵，主要面向商业级应用，IDE 的价格则较低，主要面向桌面式计算机。

易用性：在 SCSI 的使用过程中，常会发生 SCSI ID 和总线终结器设置错误，导致硬件不能识别的情况。而 IDE 设备则仅有主、副之分，在同一数据线上只有两个设备，分别将其设置为 Master 和 Slave，就不会发生冲突。

扩展性：SCSI 的优点之一是能够连接多达 15 个设备，而标准计算机的 IDE 接口，最多也只能连接 4 个设备。购买产品时，我们最先要考虑到自己的需求。如果玩游戏、看 DVD、

上网，IDE 硬盘已能满足你的应用，SCSI 仅会让 Quake 3 增加几帧，有点大材小用。若是用计算机来进行捕捉视频、编辑影像等要求大量磁盘进行输入/输出的工作，SCSI 则非常符合要求。

（5）SCSI 的未来

SCSI 是一种不断发展的技术，最近加入的规格有 Fibre Channel SCSI、IEEE 1394（Firewire，火线）和 SCSI 3（160MB/s），SCSI 4（320MB/s）和 SCSI 5（640MB/s）。从 SCSI 3 开始，SCSI 能按照需要快速地提高性能，并拥有近乎完美的向后兼容性，保护了用户的投资。随着日益提升的速度之外，SCSI 也开始注重易用性，采用 CAM（Common Access Model，公共存取模型）在众多 SCSI 命令集和程序调节之间加入了一个控制层，使 SCSI 的编程更为方便。

3.5.2 USB

USB 是一个外部总线标准，可使计算机及外部设备直接连接和通信。USB 支持即插即用、热插拔功能。USB 可用于连接 127 种外围设备，如鼠标和键盘，调制解调器等。USB 是在 1994 年年底由英特尔、康柏、IBM、微软等公司联合提出，自 1996 推出以来，已成功取代串行和并行端口，并成为个人计算机和大量智能设备必须配备的一个接口。从 1994 年 11 月 11 日公布的 USB V0.7 版本以来，V0.7 版本经历了多年的发展，现在已发展到 3.0 版。

（1）USB 的发展

1）USB 1.0。USB 1.0 是在 1996 年出现的，速度只有 1.5Mbps；1998 年升级为 USB 1.1，速度大幅提升到 12Mbps，在许多旧设备上还配置有这种标准的接口。USB 1.1 是较为普遍的 USB 规范，其高速传输速率可以达到 12Mbps，低速传输速率为 1.5Mbps。大部分 MP3 都配置有此类接口类型。

2）USB 2.0。USB 2.0 规范是由 USB 1.1 规范演变发展而来的，其传输速率达到了 480Mbps，折算为 MB 为 60MB/s，能够满足大多数外部设备的速率要求。USB 2.0 中的“增强主机控制器接口”（EHCI）定义了一个与 USB 1.1 相兼容的架构。它可以用 USB 2.0 的驱动程序驱动 USB 1.1 设备。也就是说，所有支持 USB 1.1 的设备都可以直接在 USB 2.0 的接口上使用而不必担心会发生兼容性问题，而且像 USB 线、插头等附件也都可以直接使用。

使用 USB 使通用打印机的速度大大提高，该接口使连接速度达到 12Mbps，比并行端口速度提高 10 倍以上，在这样的速度下打印文件传输时间大大减少。USB 2.0 进一步将接口速率提高到 480Mbps，是普通 USB 速度的 20 倍，更大幅度地降低了打印文件传输时间。

3）USB 3.0。由英特尔、微软、惠普、德州仪器、NEC、ST-NXP 和其他行业巨头组成

的 USB 3.0 Promoter Group 宣布，该组织负责开发新一代的 USB 3.0 标准已正式完成并公布。USB 3.0 理论速度达到 5.0Gbps，但实际上只能达到理论值的一半，但也是接近于 USB 2.0 的 10 倍了。USB 3.0 物理层使用的 8b/10b 编码，这样做的理论速度为 4Gbps，实际速度将扣除协议开销，所以实际上比 4Gbps 还要少。它被广泛应用于计算机周边设备及消费电子产品。

USB 3.0 在实际应用中，被称为“超高速 USB”，遵守先前的 USB 1.1 FullSpeed 和 USB 2.0 HighSpeed。

（2）USB 的优点

USB 设备被广泛使用，主要因为具有以下优点：

1）可热插拔。允许用户使用外部设备时，不需要关机后才能连接并行或串行电缆，而是在使用计算机工作时，直接可以插入 USB 插头。

2）携带方便。USB 设备的主要优点是“轻、小、薄”，对于用户来说，与大容量的硬盘相比，USB 硬盘要比其他类型的硬盘质量更轻，当要随身携带大容量硬盘时，USB 硬盘自然是第一选择。

3）标准统一。在出现 USB 接口之前，通常是 IDE 接口的硬盘，串行的鼠标键盘，并口打印机扫描仪。但出现 USB 接口后，这些应用外部设备都可以使用相同标准与个人计算机连接，即 USB 外置硬盘、USB 鼠标、USB 打印机等。

4）可连接多个设备。在个人计算机上往往具有多个接口，可以同时连接多个设备，如果连接上一个四端口的 USB 集线器，甚至可以连接更多的设备，例如可以将家里的所有设备也都连接到个人计算机上，而不会出现任何问题，最多可以连接 127 个设备。

（3）接口布置

USB 是一种常用的计算机接口，只有 4 根线，两根电源两根信号，故信号是串行传输的，USB 接口又称为串行口，USB 2.0 的速度可以达到 480Mbps。可以满足各种工业和民用需要。USB 接口的输出电压和电流是：+5V，500mA。实际上有误差，最大不能超过±0.2V 也就是 4.8～5.2V。USB 接口的 4 根线一般是按图 3-9 进行分配的，需要注意的是千万不要把正负极弄反了，否则会烧掉 USB 设备或者计算机的南桥芯片。黑线：GND；红线：VCC；绿线：+D；白线：−D。USB 图标和 LOG 如图 3-10 所示。

（4）接口种类

1）USB A 型公口（见图 3-11）。随着数字设备的使用越来越广泛，我们周围的 USB 设备也逐渐多了起来。然而，这些设备的尽管都使用了 USB 接口，但这些设备的数据线端口并不完全相同。这些数据线连接计算机的一端都是相同的，但连接外设的端口却因为体积的考虑各不相同。

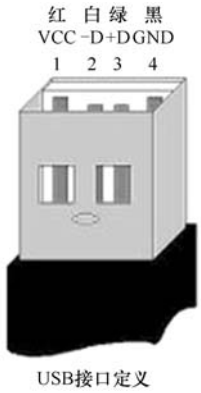


图 3-9　USB 接口定义图



图 3-10　USB 图标和 LOG



图 3-11　USB A 型公口

2）Mini B 型 5Pin（见图 3-12）。这种接口可以说是最常见的一种接口了，这种接口由于防误插性能出众，体积也比较小巧，所以正在赢得越来越多的厂商青睐，现在这种接口广泛用于读卡器、MP3、数码相机以及移动硬盘上。

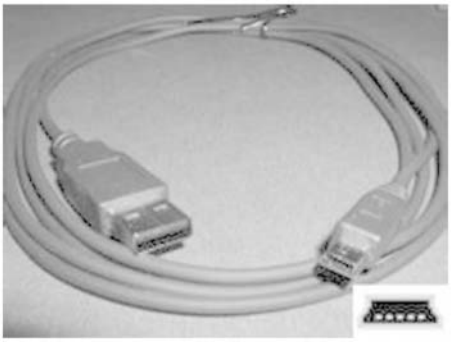


图 3-12　Mini B 型 5Pin

3）Mini B 型 4Pin（见图 3-13）。这种接口常见于以下品牌的数码产品：奥林巴斯的 C 系列和 E 系列，柯达的大部分数码相机，三星的 MP3 产品（如 Yepp），SONY 的 DSC 系列，康柏的 IPAQ 系列产品。



图 3-13　Mini B 型 4Pin

Mini B 型 4Pin 还有一种形式，那就是 Mini B 型 4Pin Flat。顾名思义，这种接口比 Mini B 型 4Pin 要更加扁平，在设备中的应用也比较广泛。

4）Mini B 型 8Pin（见图 3-14）。这种接口和前面的普通型比起来，就是将原来的 D 型接头改成了圆形接头，并且为了防止误插在一边设计了一个凸起。

这种接头可见于一些 Nikon 的数码相机，CoolPix 系列比较多见。虽然 Nikon 一直坚持用这种接口，但是在一些较新的机型中，例如 D100 和 CP2000 也都采用了普及度最高的 Mini B 型 5Pin 接口。

5）Mini B 型 8Pin 2×4（见图 3-15）。这种接口也是一种比较常见的接口，例如我们熟悉的 iRiver 的著名的 MP3 系列，其中号称“铁三角”的 180TC，以及该系列的很多其他产品采用的均是这种接口。这种接口的应用范围也较广，不过从 iRiver 自 3XX 系列全面换成 Mini B 型 5Pin 的接口后，这种规格明显没有 Mini B 型 5Pin 抢眼了。



图 3-14　Mini B 型 8Pin



图 3-15　Mini B 型 8Pin 2×4

3.5.3 SATA 接口

SATA（Serial Advanced Technology Attachment，串行高级技术附件）接口也被称为串行 ATA，SATA 接口的硬盘也叫串口硬盘，它最终将取代 IDE 接口的并口硬盘。

SATA 接口的历史：2001 年，英特尔、APT、Dell、IBM、希捷、迈拓几大厂商组成的 Serial ATA 委员会正式发布了 Serial ATA 1.0 规范。在 2002 年，虽然串行 ATA 设备尚未正式上市，但 Serial ATA 委员会已首先建立了 Serial ATA 2.0 规范。Serial ATA 使用串行连接方式，串行 ATA 总线使用嵌入式时钟信号，具有较强的纠错能力，与以往相比最大的区别在于具备对传输指令（不只是数据）进行审查的能力，如果发现错误自动校正，因此大大提高了数据传输的可靠性。串行接口还具有结构简单、支持热插拔等优势。

串口硬盘完全不同于并行 ATA 的新型硬盘接口类型，由于采用串行数据传输而广为人知。与并行 ATA 相比，它有如下许多优点。

（1）高传输率

Serial ATA 连续串行方式传输数据，一次只会传送 1 位数据。这将减少 SATA 接口的引脚数量，连接电缆少，更有效率。事实上，Serial ATA 只有 4 支引脚就可以完成所有的工作，可用于连接电缆，与接地线连接、发送数据和接收数据，这种结构还可以降低系统能耗，降低系统的复杂性。其次，Serial ATA 起点高，发展潜力很大，Serial ATA 1.0 定义的数据传输率可以达到 150MB/s，比并行 ATA（即 ATA/133）所能达到 133MB/s 最大数据传输率高，而在 Serial ATA 2.0 数据传输速率可以达到 300MB/s，最终可以达到 600MB/s 的最大数据传输速率。

（2）数据更可靠

在校准方面，并行 ATA 总线是对 CRC 进行一个简单的检查，一旦发现数据的传输问题，将会丢弃这些数据，要求重新发送，如果数据信号相互干扰太大，将严重影响硬盘的性能。串行 ATA 对 CRC 和数据分组进行校验，以提高总线可靠性。

（3）连线更简单

在数据线方面，并行 ATA 接口使用一个 80 针排线，串行 ATA 由于采用点对点方式传输数据，所以只需要 4 条线就可以完成完整的发送和接收功能，加上另外三个接地线，总共只有 7 个物理线路就能满足需要的数据传输。由于数据传输线少，使得数据在物理线路的电气性能方面的干扰减少，这将确保未来进一步提高磁盘传输率。比起并行 ATA，串行 ATA 数据线更细，这也使得机箱内部连接易整理，有助于机箱内部空气的流通，对机箱内部散热好。同时，串行 ATA 接口使用非排针脚设计，支持热插拔等。

3.5.4　IDE 电子集成驱动器

IDE（Integrated Drive Electronics）指的是并行 IDE 接口（PATA 接口），利用并行接口的硬盘被称为并口硬盘，是一种较老的技术，现在则基本不再使用此类接口硬盘。此类接口硬盘的接口连接比较简单，只需要一个 40 线电缆与主板或接口卡连接即可。盘体和控制器集成在一起的做法减少了硬盘接口线的数量和长度，数据传输的可靠性提高了，硬盘制造更简单，因为厂家不需要担心自己的硬盘和其他厂商生产的控制器是否兼容，对用户而言，硬盘安装更方便。尽管有这些优点，但其最大传输只有 133MB/s，远远低于串行接口的 600MB/s 的速度，且其他方面的性能不及 SATA 串行接口。

串行 ATA 的优势是非常明显的，SATA 接口已越来越受到欢迎，但仍有一些速度较低的设备还在使用并行 ATA，如光驱、刻录机等设备，对于这些设备，并行 ATA 传输速率已经能够满足需要。因此，并行接口和串行接口会在很长时间内共存。

3.6　结构与散热设计

3.6.1　电子产品结构设计的一般要求与原则

（1）电子产品结构设计一般要求

1）功能要求。电子产品和其他机械产品一样，在结构设计上必须满足功能要求。这体现在工作原理的实现以及工作可靠度上面。

2）产品质量要求。质量决定产品的竞争力。质量要求的具体表现有很多，包括外观、运营成本、安全、环保和其他许多要求和限制。与功能要求相比，质量要求更体现在细节上，在结构设计开始时应该纳入考虑范围。

3）结构优化要求。结构设计过程中，要实现一般功能的结构很容易设计，难在在众多结构方案中找到问题的最优解。结构优化设计应建立在材料、工艺、连接方式、形状、位置、大小和其他设计元素的综合因素基础上。

4）结构创新要求。现代电子产品迅速发展变化，市场竞争越来越激烈，逐渐向个性化要求趋近。只有包含了创造性思维的结构设计，才能使产品在竞争中立于不败之地。

（2）电子产品结构设计一般原则

1）实现所需功能的原则。电子产品的结构设计要从整体考虑其功能要求。结构组成部分的主要功能是保护电路和电路元件，承担负荷，传递运动和动力，保持相关部件之间的相对位置或运动轨迹等。通常设计师会将功能分解，得到一些子功能。不同的子功能由不同的结构部件组成，各结构间要保持和谐、合理的关系。为了简化结构，降低加工成本，

安装方便，有时一个组件可以具有多个功能。

2）满足强度和刚度的原则。在现代电子产品市场上，尤其是在消费电子产品领域，外壳材料大多采用工程塑料。普通住房虽然材料无特殊要求，但也还要通过测试要求，如环境测试、跌落试验、弯曲试验、疲劳试验等。在许多情况下，设计决定结构强度。例如，增加厚度壳体，在壳中加筋，都是提高强度的办法，但只单一增加壳体厚度是不明智的方式。要使塑料厚度尽量均匀，应避免局部强度过小而降低整体强度。减少应力集中，改善受力情况也可以非常有效地增加强度。此外，确保产品在保质期内实现其功能，必须要使产品有足够的强度。

3）满足制造工艺和装配要求的原则。电子元器件产品的设计应使其容易加工。如果产品销量较大，机械加工方式肯定是不适宜的。结构组件中的外壳、按键等，通常采用注塑成形的办法。相反，如果是小批量生产，则使用模具生产是不经济的，因为模具制造的成本较高。装配产品性能也是衡量产品结构设计的成功或失败的因素之一。结构设计要合理划分装配单元，使结构组件被正确安装。

4）符合审美要求的原则。现代电子产品的外观提出了更高的要求，先进的制造技术和表面处理方法也对各种造型形状提供有力的保障。结构设计师在考虑充分满足功能要求的同时，也要配合工业设计师，使产品的外观符合大众要求。

结构设计是电子产品设计的重要组成部分，合理的结构必须是根据一定要求进行设计的，如图 3-16 所示。只有充分认识电子产品结构设计的一般要求和结构设计的原则，大胆假设，小心证明，才可以设计一个满意的产品。

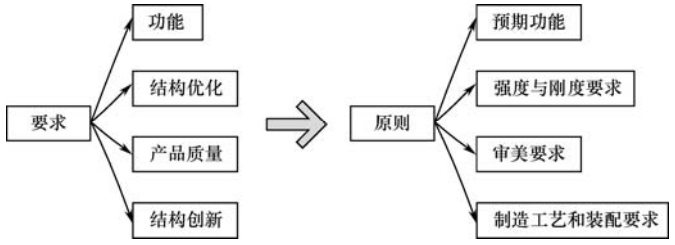


图 3-16　电子产品结构设计的一般要求与原则

3.6.2　电子产品的结构设计过程

（1）ID 造型

交互设计（Interaction Design，ID）。从用户的角度来说，交互设计是一种如何使产品使用方便，高效并且使人愉快的技术，它致力于了解目标用户和他们的期望，了解用户与产品交互时的行为，了解“人”的心理和行为特征，同时也包括了解各种有效的互动模式，并加强与扩展。互动设计涉及多个学科和领域，以及多背景多专业人员之间的交流。通过

产品界面与用户行为的互动设计，使产品和使用者之间建立有机联系，有效地实现用户的目标，这是互动设计的目的。

一个完整的产品设计过程中，一般从造型开始，收到客户的原始数据（这可能是草图，也可以是文字说明），开始形状设计；ID 工程师绘制符合要求的外壳，交客户确认，逐步修改，直到客户认同；也有的公司是 ID 工程师画几个草案，由客户选择一个，ID 工程师在此基础上完成草图轮廓图；图的类型，可以是二维工程图，包括必要的投影视图；也可以是其他格式的图片。无论哪一种，一般需要指定尺寸。其他方面的要求，比如表面处理工艺，颜色等需要求根据实际情况确定。

外形确定后，接下来的工作是结构设计工程师的工作，包括信息核对，提供一个完整的电子解决方案等。

（2）建模阶段

结构设计工程师根据 ID 工程师提供的信息绘制基本形状，基本形状就像是基石，所有的表面结构部件都以它作为参考。ID 工程师侧重造型，不必理会拔模角度，而结构设计工程师不但要做出拔模角度，还要知晓各部件的装配关系。

具体做法是：先导入 ID 工程师的文件，尊重 ID 工程师的设计意图，不能随意改变；画线，PROE 是参数化设计工具，扫描线的目的是方便测量和修改；画曲面时要和实体一致，这也是后面进行图形拆分的基础。装配图绘制时，把拆分后的各个结构部件按照顺序依次绘出，选择参考中心对准的对齐方式。放入各个电子零部件，如液晶显示器、发光二极管、电池等，并引入装配图，也可根据需要将某些零部件先组成一个组件，再将组件引入装配图。

（3）初始造型阶段

1）造型工程师设计出产品的整体造型，也可提供多种方案由客户进行选择或客户自主开发。

2）客户提供设计资料。

3）在原有的外形基础上更改；也可提供多种方案由客户进行选择或客户自主开发。

（4）检查元件的位置

对各元件的位置进行检查，一般元件的摆放是有各自严格位置要求的。

（5）完善

就像大楼的框架已经构建好了，现在可以依托框架由下而上，完善每一个楼层了。

3.6.3　散热设计

目前电子产品零部件的集成度越来越高，印制电路板上的电子元件密度也越来越高。因为电子产品日益小型化和更薄，很难依靠外壳设计出高效冷却印制电路板上的电子元件

的通道。可以说电子元件容易发热，但散热冷却却很难。从电子元件到印制电路板和机壳，根据各部分的热特性设计散热路径，使热量从每个电子元件毫无保留地散热，这样的设计与技术越来越重要。

苹果公司为了解决 Mac-Book Air 新机型的空气散热问题花了很多努力。

第一代 Mac-Book Air 机型已经出现过这样的问题，即当处理负担加重时，配备的双核微处理器内核将停止工作，从而导致计算机运行慢。虽然这个问题被认为是防止热失控现象的“措施”，而不是一个缺陷，但苹果公司仍然更新了这个机型的固件。

苹果公司自认为通过更新固件的措施解决了散热问题，但又出现了新的问题。虽然内核不再停止工作，但计算机会频繁发生启动“kernel_task”的高负荷的任务。kernel_task 是防止过热而采用的进程。双内核的总处理能力为 200%，而 kernel_task 的处理能力却占到了 130%～150%。越来越多的用户对繁重的处理负担表示不满。因此，苹果公司采取了许多措施。

第一，选择合适的中央处理器。11 英寸的型号就选择了“SU9400”，其工作频率低，被称为“超低电压型”。工作频率从第一代机型的 1.6GHz 降到了 1.4GHz。

第二，制造工艺也发生了变化。尺寸从 65nm 降低到 45nm。也起到了积极的作用，热设计功耗（Thermal design power，TDP）从第一代机型约 20W 降低了约一半。从减少热量的角度来看，这是一个合理的选择。

此外，还配备了一个以前未使用的散热管，从而提高散热效果。还有在外壳上粘贴石墨散热片，从而加快散热。

第 4 章　物体特征数据的传输与路由

4.1　数据中心式路由

4.1.1　数据中心式路由协议

无线传感器网络一般对信息感兴趣，但不对信息来源感兴趣。因此无线传感器网络是以数据为中心进行交互。信息发送到接收器，接收器判断对该信息是否感兴趣，从而决定是否接收信息，而不是以发送者的地址为目的。在数据中心式模式下，信息接收器不关心数据来源，并且发件人也只是简单地发送数据。以数据为中心路由协议是实现这种互动模式的一种形式。以数据为中心的路由机制，提出以数据的内容（如结点信息、查询的内容或转发的信息）来区分结点。以下介绍几种典型的无线传感器网络以数据为中心的路由协议。

（1）基于信息协商的路由协议 SPIN

SPIN 是第一个以数据为中心的自适应路由协议，它是通过结点之间的协商来减少网络中的数据传输数量。SPIN 首先提出元数据（meta-data）的概念，元数据是对结点感知的数据的抽象描述。元数据对于数据本身来说非常小，所以在协商过程中不会消耗太多结点的能量，如果元数据和数据本身差别并不大，那么协商就失去了它的意义。元数据的概念是一种变相的感知数据压缩包，需要协商的是哪些元数据应该发送到目的结点。SPIN 基本上是洪泛算法的升级，为解决泛洪算法的不足，引入了结点之间的协商机制和资源自适应机制。传感器结点的数据传输给对方之前需要事先协商，协商机制可以确保传输的是有用数据。

SPIN 协议有 3 种数据包类型，采用三次握手来实现数据交互，即 ADV、REQ、DATA。

ADV：用于数据广播，其中每个 ADV 数据包含元数据信息。

REQ：用于请求发送数据。

DATA：原始感知数据包，具体过程如图 4-1 所示。

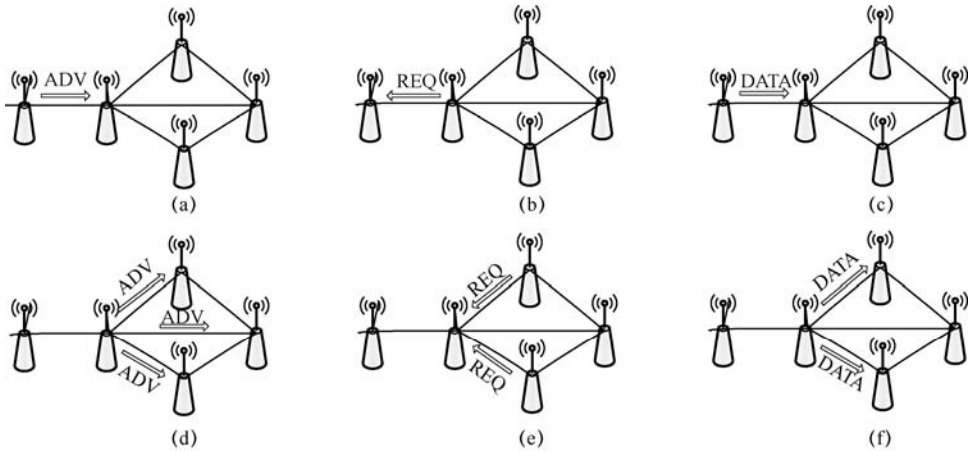


图 4-1　SPIN 协议基本过程

传感器结点监测到一个事件，要做的第一件事是向其邻居结点广播包含元数据的 ADV 数据包，如图 4-1（a）所示。相应的邻居结点接收到 ADV 数据包后，检查自己是否有 ADV 描述的数据，如果没有，那么它向发送 ADV 的源结点发送一个 REQ 数据包，如图 4-1（b）所示。然后数据源结点向该邻居结点发送 DATA 数据包，如图 4-1 所示（c）。接收数据的邻居结点也重复同样的步骤，发布该数据的元数据以告知其邻居结点，如图 4-1（d-f）所示，使 DATA 数据包可以传送到远程结点。

SPIN 协议用协商的方法达到有目的的转发，它使用以下三个步骤实现数据传输。

1）获取新数据的结点通过传感器或通过其他结点向其邻居结点通告数据名称。

2）接收到通告信息的结点将接收信息与本地信息进行比较，如果通告信息对于本地信息是未知的，接收结点就发送数据请求；如果通告信息是已知的（例如，它已经通过其他途径或结点接收这一地区报告的数据），那么这个通告信息就可以忽略。

3）只有在收到结点发送的数据请求后，结点才发送实际的数据。

SPIN 协议的好处在于描述数据的大小与数据本身的大小相比显得非常小。当描述数据和数据本身大小相近，使用事先发送通告信息而非直接发送实际数据就没有意义了。其优势是在实际数据的基础上，可以在网络内限制数据的泛洪。SPIN 协议拥有比广播结构更强大的结构，因为它考虑到了数据丢失和多个结点不报告数据（可能是多余的数据）的情况。

SPIN 协议还有某些其他形式的变化，可以使结点的行为模式适应结点的剩余能量。在发送或接收数据之前，每个结点都必须检查各自可用的能量状态。如果结点的剩余能量低于某个阈值，那么它不参加任何消息转发，只接收来自邻居的报文和自己的请求消息发送。

（2）基于交互的定向扩散协议 DD

定向扩散算法是专为无线传感器网络设计的，以数据为中心，基于查询的路由算法。

定向扩散算法中包含了两个基本概念：兴趣和梯度。在定向扩散算法 DD 中，汇聚结点定期通过泛洪的方式广播兴趣消息到整个网络。这个兴趣消息通知网络中的传感器结点，告诉它们汇聚结点需要收集哪些类型的数据。通过兴趣消息在网络中逐跳传输，从源结点到汇聚结点就建立了数据传输梯度。

定向扩散对数据有其独特的命名方式。它的兴趣和事件是通过属性名称、属性值的方式来命名的。在同一个应用中，使用类似或相同的命名机制，易于识别匹配处理。

定向扩散算法 DD 分为兴趣扩散、梯度的建立及路径加强三阶段，如图 4-2 所示。

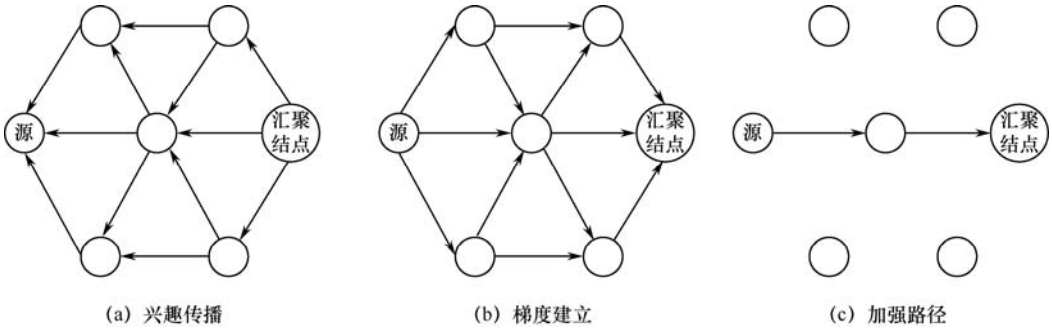


图 4-2　定向扩散算法基本流程

第一阶段是有兴趣扩散阶段：如图 4-2（a）表明，汇聚结点将任务以兴趣消息的形式，广播多跳的方式，定期发送到每个邻居结点。一般来说兴趣消息包含任务类型、目标区、数据传输速率、时间戳等参数描述。每个结点维护一个自己的兴趣列表，用来缓存每个收到的兴趣消息，然后将每个兴趣消息都以列表的形式记录传播信息的邻居结点和时间戳等信息，从而建立结点间的梯度。这样，随着兴趣通过网络传输，数据从源结点到目的结点建立数据传输梯度。每一个兴趣都有各自的生存时间，超过有效期，这种兴趣就消失了，结点将这种兴趣消息删除。一个兴趣消息可能由多个邻居结点传送，因此各兴趣消息可对应多个邻居结点，但每个邻居结点只对应一个梯度信息。

当一个结点收到一个邻居结点的兴趣消息时，第一个结点检查您的兴趣清单是否有相同的兴趣。如果有，则更新兴趣列表中该兴趣消息的有效时间值；如果没有，则为这个兴趣消息重新建立兴趣表项，表项中建立了一个独特的梯度与这个邻居结点相对应。一个兴趣表项可以有多个梯度域，但每个梯度域只对应转发该兴趣消息的邻居结点。

第二阶段是梯度建立阶段，如图 4-2（b）所示。事件源结点接收到兴趣消息时，对这个兴趣消息作出响应。回应的报文消息通过不同的路径到达汇聚结点。

第三阶段是路径加强阶段，如图 4-2（c）所示。汇聚结点收到从源结点发出通过不同路径传输的数据后，根据路径加强机制启动从汇聚结点到源结点的加强路径，以后的数据将

沿该路径传输。图 4-2（c）中的路径加强标准有很多，如选择数据传输延迟的标准，当汇聚结点接收到一个新的数据，它就将发送最新数据的邻居结点作为加强路径的下一跳结点，向它发送路径加强消息。邻居结点在收到消息时，判断此消息是一个路径加强信息，并更新相应的兴趣表项到邻居结点的传输速率等参数。同理，按照同样的规则来加强路径的下一跳邻居结点。具体的路径加强准则，可以按照各种应用需求选择适合的方案。如对数据传输稳定性要求高的应用可以选择数据传输最稳定的结点作为路径加强的下一跳结点。

定向扩散算法是一个经典的以数据为中心的路由算法。汇聚结点周期性的洪泛兴趣数据包里包含了任务类型、目标区域等参数。中间传感结点通过兴趣数据包建立起从数据源到汇聚结点的数据传输梯度，形成从汇聚结点到目的结点的多条数据传输路径。再按照某个特定的路径加强标准，生成一条加强的数据传输路径。无线传感网络的拓扑结构等是变化的，所以定向扩散算法要周期性地进行兴趣广播、数据广播和路径加强三个手段来维持路由的有效性和适应网络拓扑结构变化等情况。

与传统的路由算法相比，定向扩散算法 DD 具有鲜明的特色，主要体现在以下几个方面：

1）以数据为中心，把兴趣和事件用属性值的方法进行描述。

2）数据传输是在相邻的结点之间进行的，每个结点不需要知道整个网络的拓扑结构。

3）每个结点需要具有进行数据处理的能力。

4）一个结点出现故障，整个路由需要重新建立。

5）兴趣扩散到泛洪方式传播，能量和时间消耗比较大。

（3）谣传路由 Rumor

传感器网络应用形式具有多样性，定向扩散算法在一些应用中不是效率最高的路由，例如在数据传输量较少或时间区域已知的情况下。因此有人在定向扩散算法的基础上提出谣传路由（Rumor routing）。

为解决定向扩散算法应用泛洪的方式建立路径代价太大的问题，谣传路由使用查询消息的单播随机转发方式。谣传路由的基本思想是：事件区域的传感器结点感知到事件后，将生成一个代理消息（agent），代理消息随机选择一个邻居结点向外传播，如图 4-3 中的黑色结点，同时从汇聚结点开始的查询消息也在网络随机传播，如图 4-3 中的灰色结点。当两类消息交叉时，形成了从源结点到目的结点的完整路径。这种方法避免了洪泛报文传输能量消耗过大的弊端，但付出的代价是延长了数据传输时间，数据包延迟时间增加。

谣传路由的主要特点如下。

1）每个结点维护一个邻居列表和事件列表。邻居列表记录结点的邻居信息，事件列表记录的是与事件有关的信息（如事件的名称、下一跳邻居等）。一个传感器结点感知事件发生时，事件列表添加一项来描述这个事件，并产生消息代理。

2）消息代理具有一定的生命周期，它将携带的信息传递给它经过的每个传感器结点，直至代理的生命周期结束。

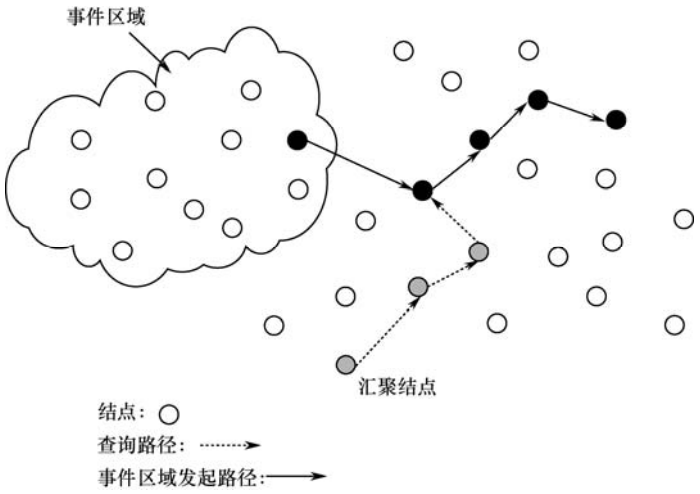


图 4-3　谣传路由基本过程

3）网络中的任何结点都可以产生对某种特定事件的查询消息，查询消息也有一个生命周期。

4）当查询消息和代理消息重叠时，重叠结点沿与查询消息相反的方向，将事件传送到查询结点。谣传路由相对定向扩散算法，可以有效地减少路由开销。然而，由于这种路由机制使用一个单播方式随机选择路径，数据延迟是相当大的。并且传输路径往往不是最好的路径，并可能出现循环路径问题。

4.1.2　以数据为中心的路由机制缺陷分析

以数据为中心路由协议是为无线传感器网络设计的，上文介绍了以数据为中心的路由机制的三个主要算法，它们都是用数据的一部分来建立路由。SPIN 发送元数据和邻居结点协商，然后发送数据；RUMOR 算法采用代理消息的形式向外转发事件，直到代理消息和汇聚结点查询消息成功交互，然后再发送数据；定向扩散算法 DD 是通过设立从源结点到目的结点的梯度，然后发送数据。三种路由机制都是使用数据的一部分，然后转发所有数据，这种方法可以有效降低能源消耗，但它们也有许多缺点。

（1）无全网统一标识

SPIN、RUMOR 和定向扩散算法 DD 都没有一个统一的全体网络标识。它们是通过数据匹配来进行互动的，这是因为无线传感器网络主要是监测区域的感知数据，而不是具体

的结点信息。但这种不具有全网标签的方式也有其自身的缺点。在这种情况下，网络中的结点无法区分不同兴趣消息是否来源于不同的结点，不清楚它们是否需要建立自己的路径。也就是说一个结点收到多个兴趣或查询，但它不能确定这些信息是由同一个汇聚结点发出还是由不同的结点发送。下面是一个定向扩散算法 DD 的例子。

如图 4-4（1）所示是来自不同的汇聚结点的兴趣通过结点转发，都到达 A 结点。图 4-4（2）所示是同一个结点的兴趣，通过不同的中间结点转发到结点 A。在这种情况下，结点 A 就无法确定兴趣消息是否来源于不同的汇聚结点，是否需要建立所有兴趣的梯度和通知所有发送数据的汇聚结点的最优路径。同时，无法确定这些数据分组属于同一个汇聚结点，还是只是通过不同的转发结点。这种无全网统一标识的特征有许多缺点，比如结点 A 遇到图中的两个情况后，就有两个极端：要么只接收一个兴趣，放弃所有重复的兴趣；要么为每一个兴趣建立梯度。在第一种情况下，结点放弃所有重复的兴趣，但这一新的兴趣可能不是来自同一个汇聚结点，这样，就无法正确建立源结点的路径加强。在第二种情况下，为每一个兴趣建立一个梯度信息，会造成很多不必要的开支。

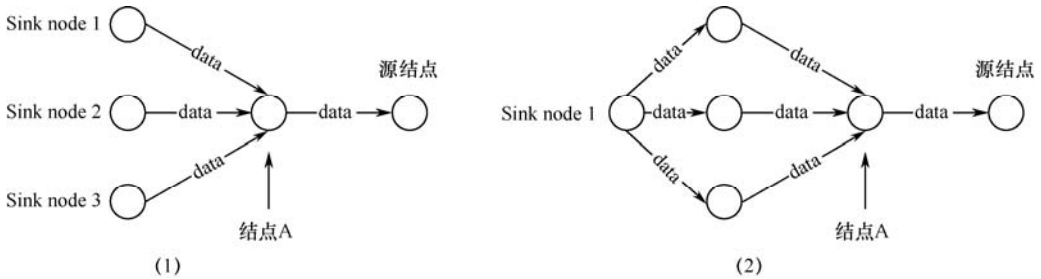


图 4-4　无全网同意标号涌现的混乱

（2）与洪泛路由的关系

我们可以看到，这三个以数据为中心的路由机制都和洪泛算法密切相关，SPIN 和 Rumor 是泛洪算法的改进。SPIN 用三步来代替简单的泛洪算法，实际上是在实际数据的基础上对泛洪做了一定的限制。当 SPIN 需要发送数据的时候，整个网络其实质是一个以数据为中心的泛洪算法。Rumor 随机发送代理信息，但不是向所有邻居广播消息。定向扩散算法 DD 在路由建立时通过泛洪算法探索网络。

（3）没有路由表和邻居表

三种路由算法是直接通过数据在网络中进行匹配，建立自己的路由表和邻居表。需要发送数据的时候，数据直接发送到他们的相邻结点，然后邻居结点经过一定的策略来传输数据。每当结点监测到一个新的事件或汇聚结点进行一个新的查询时，都需要一个路由发现过程，数据延迟比较大。

三个数据为中心路由机制，除了较常见的共同缺点外，也有自己的缺点。SPIN 的缺点是 SPIN 的应用有一个假设，假设每个传感器结点都向结点发送数据，并且每个结点的数据是比较大的。这样结点拥有的每一部分数据很容易获得一个唯一的名称，这个名称对于数据来说很小。如果数据名称和数据本身在大小上没有太大的区别，它将失去协商的意义。Rumor 的缺点是 Rumor 只适合网络数据传输量很少的情况，它的数据延迟是相当大的，且通过随机生成的路径，因此不可能产生最优路径，并且环路问题也很严重。定向扩散算法 DD 的缺点是定向扩散算法在路由建立时需要一个兴趣扩散算法，能量和时间开销比较大。

无线传感器网络是以数据为中心的网络，它的这个特点使它迫切需要一个以数据为中心的路由协议支持，这类协议虽然基本上可以实现路由功能，但缺点是不能忽视的。

4.2 集群结构式的路由

路由器集群，也被称为路由器矩阵或机框互联（Multi-chassis），简单地说，就是多个路由器相互连接，形成了一套逻辑集成路由器系统。集群技术的出现主要原因有两点：首先，单机容量逐渐发展到极限，成为网络发展的瓶颈；其次，超级结点使网络结构日趋复杂，大大提高了管理的难度，增加了经营成本。

集群技术通过集中化综合控制管理，使路由器集群系统之间的单机能很好地在一起工作，通过不同的组织形式可以无限扩展路由器的能力，从而打破了单机对技术的制约。同时，由于集群系统的每一个路由器通过高速光背板互联，节省了额外的内部互联网端口，从而大大降低对网络硬件设备的投资。更为重要的是，由于集群路由器对外体现为单一路由器，网络具有结构简单、清晰的特点，为各种商业设计软件的路由策略提供便利条件，大大降低了维护难度，节约运行费用。

4.2.1 集群技术的组织形式

根据集群设备数量的不同，路由器集群结构可以分为两框集群、四框集群和多框集群。从目前的实现技术来看，集群中多个设备之间的连接是使用对等互连或中心交换框技术，通过建设类似 HUB-SPOKE 的方法来实现。因此，集群的具体结构可分为背靠背、1 托 m、2 托 m 和 n 拖 m。“背靠背”是指两个用户框直接连接，不通过中心交换框；“1 托 m”是指 m 台用户框通过 1 台中心交换框集群；“2 托 m”是指 m 台用户框通过两台中心交换框集群。随着科学技术的发展和不断进步，未来集群的具体结构将朝着“n 拖 m”发展，“n 拖 m”的结构将使集群路由器的数量达到 64 框以上，系统容量可达到 100T 以上。

由于集群内设备之间的数据交换量巨大，采用传统的光纤互连已远远满足不了级联的

需求。因此，需要采用专用的大容量数据光纤带进行互联，但由于工艺复杂，大容量数据光纤带的成本也相对较高。目前大容量数据光纤带可做到每束光纤带包含 72 芯 2.5G 的光纤，每束光纤带的传送能力可达 180G/s。从业界技术水平的发展来看，目前两框集群技术已经具备商用能力，四框及多框集群也将逐步成熟。对于两框集群技术，又可采用“背对背”、“1 拖 2”及“2 拖 2”三种方式来实现，图 4-5 所示为两框集群的实现方式。

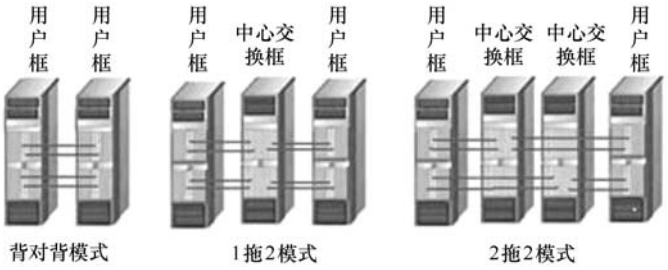


图 4-5　两框集群的实现方式

4.2.2　集群技术的交换结构

路由器的核心技术是交换结构，它直接决定了整个系统的性能。在介绍交换方式之前，绝大多数路由器都采用共享总线分布式处理技术。共享总线的实现比较简单，但由于无法避免内部冲突，使高速总线的设计受到限制，并且变得越来越困难。交换技术借鉴 ATM 交换机的各种优势，很好地解决了共享总线缺乏的问题。一直以来，设备商和应用商都在研究和寻找更有效的交换方式，以解决交换过程的冲突问题。

交换结构又分为单级交换和多级交换两种。

（1）单级交换

目前使用较多的单级交换结构有共享内存和 Crossbar 两种。

共享内存结构通过共享输入和输出端口存储器件，减少了对总体存储空间的需求。分组交换通过指针调度实现，提高了交换容量。共享内存结构相对简单，交换效率可根据需求不断优化。共享内存交换结构的交换性能取决于共享内存的存取速率，可扩展性较差，尤其当板卡端口数量较多时，交换效率有所下降。并且共享内存的稳定性一般，也直接影响了整个交换体系。

Crossbar 是一个严格无阻塞交换结构，输入和输出之间可以建立多个路径。Crossbar 交换结构分为集中式（输入>输出）、扩展式（输入<输出）和连接式（输入=输出）3 种。典型的 Crossbar 使用连接式，即 N×N 的交叉矩阵。Crossbar 用调度器，根据每个输入点的相关信息、运行调度算法使输入和输出匹配，并配置相应的交叉点。其中调度器效率是关键，它决定了交换速率，进而影响调度算法。

共享内存和 Crossbar 属于单级交换结构。单级交换结构由于技术限制，可扩展性是不完善的，也无法回避仲裁机制，容易成为瓶颈。因此，单级交换结构不是未来的大容量路由器发展方向，要逐步扩展到多级交换结构。

（2）多级交换

多级交换通过多个独立的交换矩阵，组成多级多平面交换矩阵。每个平面配置独立的仲裁器以避免仲裁器的瓶颈问题。多级交换大大提高系统容量的扩展性，现在大多数路由器集群都是基于多级交换结构。

多级交换结构的单位称为交换单元，每个单元都有一个输入和输出功能。每个单元通过一个逻辑顺序相互连接，形成一个大的可扩展的交互网络。多级交换结构有多种形式，包括 Clos、Banyan、Butterfly 和 Benes 等，各种不同的交换结构具有不同的互联方式。多级交换结构可分为阻塞和无阻塞两种，其中无阻塞交换分为严格无阻塞、可重排无阻塞和广义无阻塞 3 种。严格无阻塞交换手段是指只要连接的起点和终点是空闲的，任何时候都可以在交换网络建立连接；可重排无阻塞网络指的是只要一个连接的起点和终点是空闲的，任何时候都可以在交换网络中直接或间接地对现有的连接重新选择路径，建立一个连接；广义无阻塞网络的定义是建立连接时按照一定的规则选择路径，也可以在任何时间建立一个连接。

4.2.3　集群路由器

集群路由器是指多个独立的路由交换结点（如传统的路由器或通用 PC），通过一些互联方式组合成的单映像路由系统。集群路由器图如图 4-6 所示，由 M 个交换结点组成，每个交换结点是一个传统的路由器或通用 PC。路由器各个交换结点之间通过互联结构（高速互连网络或高速交换结构）连接在一起。

通过定义，我们可以看出，集群路由器不是一台路由器或计算机，它是一群计算机组合起来，由某种控制机制来协同工作。集群路由器不仅能完成常规路由器的一切功能，而且由于它是多台主机共同工作，它的可扩展性、可用性等都优于常规的路由器。

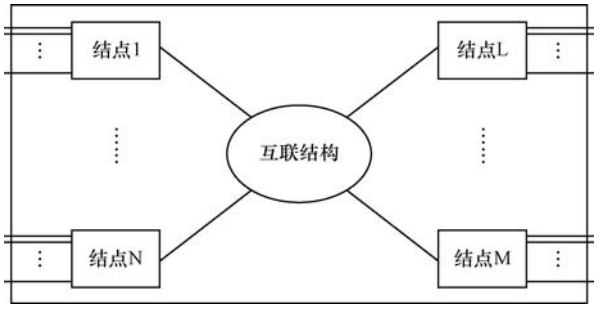


图 4-6　集群路由器示意图

根据集群路由器的定义，集群路由器的构成结点以及关键特征必须满足：

1）集群路由器在物理结构上由多个路由交换结点组成，每个交换结点包含独立的报文转发引擎和控制平面的计算资源。例如，交换结点可以是基于分布式转发结构的高性能路由器，也可以是一台通用 PC。前者的报文转发引擎对应于 ASIC 芯片或者网络处理器，后者的转发引擎只是软件系统的一个模块。每个交换结点既可以独立的执行协议计算、报文转发功能，又可以在集群软件的配置下以协同方式进行分布式的报文转发，可用性强。

2）多个路由交换结点通过某种互联方式连接起来，构成高性能的集群结构。在定义中对互联方式没有任何约束，它可以是高速交换网络，也可以是光交换设备，甚至是具有一定拓扑结构的局域网络。由于单播和组播等转发协议的需要，内部互联方式必须支持单播、广播、组播等灵活的网络内部传输机制。

3）组成集群路由器的路由交换结点可以是同构的，也可以是异构的。这里的同构性、异构性包含两方面的含义：在硬件组成上，路由结点的同构性要求每个结点具有相同的硬件配置和处理能力，异构的路由结点则可以是多种网络设备、PC 的混合。在路由软件上，路由结点的同构性指结点之间具有对称的软件功能，每个结点在不需要其他结点协助的情况下能够独立地完成全部软件功能；异构性指每个结点负责整个路由软件中一个或者部分模块的执行，只有全部结点集合才能完整地代表整个路由软件系统。

4）集群路由器必须保持单映像性。单映像性是指从组网的角度来看，一个集群路由器是一台路由器，而不是一个具有拓扑结构的网络。即从集群路由器所在网络中任意一个路由器（不包括集群路由器自身）的视图来看，集群路由器应该表现为网络拓扑中的一个路由结点，而不是具有拓扑结构的子网，因此它具有良好的可管理性。

4.2.4 集群路由器分类

（1）按控制平面分类

路由器的基本功能是路径的选择（即路由）和分组转发，路径选择功能是由控制平面完成，因此研究控制平面具有重要意义。根据集群路由器控制平面的不同，集群路由器分为两大类：集中式控制集群路由器和分布式控制集群路由器。

1）集中式控制集群路由器。

早期很多集群结构的大规模并行路由器系统，使用传统的集中式控制结构完成路由计算功能。中央集中控制结构实际上是将传统的路由器软件在不改变该软件的基础上直接移植到集群路由器体系中。通常在许多结点集群路由器的结点中指定一个高性能结点为中心控制结点，负责执行用户接口模块、网络管理模块、路由协议模块的核心功能，而其他结点都集中在报文转发操作。尽管不同的集群路由器控制平面的实现方式千差万

别，但中央集中控制模式的核心特征是路由协议和路由表的计算只集中在集群路由器一个结点来完成。

根据路由结点配置数也可以把集中控制式集群路由器分为两大类：无冗余的集中控制集群路由器和冗余集中控制集群路由器。后者将增加收购成本，但可靠性比前者更明显，因此目前的商用高性能核心路由器使用多冗余控制结构。冗余控制集群路由器可以提供高可靠性，但不能使用分布式计算资源加快软件系统。

pluris 并行路由器是一个典型的集中控制模式。pluris 系统可以指定一个或多个高性能的结点作为路由服务器，其他处理结点在收到路由信息时，只是把路由信息转发到路由服务器上。路由服务器代表其他处理结点计算路由信息，完成计算后，将新消息转发到所有转发结点。转发结点将这些信息存储在一个转发表中，并转发消息。使用多个路由服务器时，每个路由服务器独立计算路由信息，并将更新消息转发到所有转发结点。AVICI 的 NSR 软件系统可以使用多个路由控制器（一个主控制器，一个备份路由控制器和一个或多个冗余路由控制器），但在正常工作状态下只有主路由控制器运行所有的软件过程，维护路由和转发表，协调和控制整个系统的运作。备份控制器和多个冗余控制器仅在主控制器失败的情况下才交替操作。这种多路由控制器结构仍属于中央集中控制模式。基于集中控制商用集群路由器系统有 Juniper 的 T640 使用的 JUNOS 路由软件系统。

2）分布式控制集群路由器。

为了提高控制平面计算能力、存储能力等可扩展性，满足路由协议和路由表计算系统在资源消耗和需求方面的快速增长，集群路由器控制平面将充分利用每个路由结点的分布式计算资源和存储资源，在控制平面软件结构上向分布并行处理的方向发展。

根据每个结点控制平面的功能是否一样，可以把分布式并行集群路由器分为两大类：对等控制功能的分布式并行集群路由器和非对等控制功能的分布式并行集群路由器。前者是指每个结点的控制平面功能相同（即运行相同路由或信令协议），后者指的是结点的控制平面功能的不同（例如一些结点运行 BGP 路由协议和结点运行 OSPF 路由协议）。日本 NNT 网络实验室 CORErouter-1 验证系统就是针对分布式控制平面体系结构进行研究。COREouter-1 是由市场上大量销售的工作站+交换网络构成的一个集群系统，工作站根据处理任务的不同分为不同的接口结点、协议结点、路由服务结点和应用服务结点。每个结点都是一个单独的 SUN SS20 工作站（SuperSparc85-MHz 处理器），通过高速 8 端口 Crossbar 交换网络互联，最大可以支持 640Mbps 的数据传输率。为保证高负荷条件下这些处理器之间可以正常通信，还可以通过以太网互联传输控制信息。

每个结点的功能描述如下。

接口结点：每个接口结点通过 Cache 存储转发表中的路由信息。当外部接口接收 IP 报文时，先在 Cache 搜索报文转发的信息，进而确定输出结点并转发报文。

协议结点：协议结点负责执行路由协议，网络拓扑结构变化时，重新计算路由。如果路由变化，通过控制网络通知服务结点更新转发表。

路由服务结点：根据协议结点的更新通知维护转发表。在接口结点 Cache 失效情况下，响应来自接口结点的查询请求，返回路由转发信息。在协议结点撤销路由时，广播 Cache 失效通知。

应用服务结点：为整个路由器提供 UI、防火墙、域名服务、代理服务等网络功能。

CORErouter-1 并行性来自两个方面：一方面是目前已经得到广泛研究的报文转发层面的软件并行转发技术；另一方面是控制平面软件功能模块间的并行。CORErouter-1 把路由表计算、路由协议执行和网络应用服务分别放置在不同的结点上，充分利用三者之间的并行性以提高控制平面的执行效率，保证三者之间的性能隔绝，提高了整个系统的可靠性。

（2）按转发平面分类

集群路由器的转发平面是由多个结点的转发平面组成的，它们之间共同协作完成数据报文的转发工作。按照集群路由器的每个结点转发平面完成的功能是否相同，可以把集群路由器分为两类：对等转发功能集群路由器和非对等转发功能集群路由器。

对等转发功能集群路由器是指路由器的每个交换结点对数据包的转发处理是一样的，而非对等转发功能集群路由器是指路由器的交换结点对数据包的转发处理是不一样的。例如某些特定的数据报文只能由个别的交换结点处理，有的交换结点负责报文内容检查、报文过滤等。针对路由器转发平面功能的可扩展性展开的研究主要有 Click、Scout 等。

Click 的设计主要针对一般软件路由器的不灵活性，提出了灵活而且完整的结构抽象。Click 根据数据包在路由器中受路由器各功能模块作用而引起的数据包内容或传输方向变化对路由器功能实施抽象，将各功能抽象成独立的逻辑功能模块，各个逻辑功能模块对数据包做单一且不冲突的处理。使用 Click 构造路由器时，用户根据自己的需求结合 Click 的抽象方法确定路由器工作时的功能模块，接着从 Click 提供的逻辑功能模块库中选取能够实现所需功能的逻辑功能模块并将各逻辑功能模块连接成图，从而构造出符合需求的软件路由器。可以看出，用户可以通过 Click 设计结点的转发平面功能，它既可以使每个结点的转发平面功能相同，也可以单独设计每个结点的转发平面功能，具有展性好、开发成本低、开放性好、并发度高、加速比大的优点。

虽然软件集群路由器具有很多优点，但是它不同于传统路由器体系结构。软件集群路由器是将路由结点组织在一起，在逻辑上形成一个单映像的统一路由系统，因此集群路由器平台面临着很多亟须解决的关键问题，其中最重要的三个关键问题是设备单一视图、协议模块迁移、转发表同步。

“设备单一视图”是指集群路由器的多个结点通过分布协同，对外呈现单一设备视图，

同时集群内部对于外部链接特性也要实现统一视图。路由结点的每个物理网络接口在逻辑上对应一个设备驱动程序，负责数据包文的接收、发送和网络接口实时状态监控。集群路由器要维护一个设备层次的单映像视图，必须将物理上分布在各个路由结点的设备网络接口映射成统一的逻辑设备视图。该视图应具有以下一些特点：

1）路由结点间内部互联卡接口不应该再作为网络接口对待，而是成为内部互连网络的一部分；

2）所有结点的对外网络接口应该在整个集群范围内进行统一编址和映射，从而在逻辑上构成完整的路由器软件系统设备驱动层；

3）该视图要能够实时反映任意一个物理网络接口的重要状态信息的变化，并在整个集群范围内进行更新维护。

“设备单一视图”是集群路由器的最基本技术之一。

“协议模块迁移”是指构成集群路由器的路由结点在计算能力和存储能力上可能是异构的，即使是同构条件下各个结点的负载情况也可能完全不同，因此软件系统必须能够按照各个结点当前的负载情况，决定协议模块在结点上的分布。当结点发生故障或者该结点的计算能力无法满足协议需求时，在不影响协议外部行为的情况下，必须能够及时地将协议模块迁移到其他空闲结点上。“协议模块迁移”是体现集群路由器在高可用性和负载均衡分布等方面的重要支撑技术之一。

“转发表同步”是指每个结点对到达相同地址的 IP 报文按照相同的路由策略进行转发。这要求集群各结点具有面向统一接口视图的相同报文转发表，即集群路由器的每个路由结点具有相同的转发表映像。在集群路由器运行过程中，路由协议与邻接路由器交换路由信息，不断地更新本地转发表数据库。因此“转发表同步”是集群路由器系统的关键技术之一。

4.2.5　集群路由器的优点

集群路由器体系结构和传统的路由器体系结构相比具有明显的优势。

一方面，和一个固定的路由器体系结构相比，集群路由器体系结构由于其分布性特点很容易获得更好的可伸缩性和可用性，容易支持更大的规模、更好的性能，更容易提供各种服务和接口，所以它可以满足新一代互联网的发展需要。

另一方面，集群路由器在网络拓扑中是一个独立的网络结点，可以减少复杂的网络拓扑结构，具有较好的可管理性。同时由于内部多个路由器结点的紧密结合，集群路由器在数据交换和路由协议处理方面可以获得较高的性能。

4.3 位置信息路由

在无线传感器网络的研究中，一个常见的应用是用户查询特定区域中的某些特征数据，而不是一个特定结点的数据。例如，用户往往发出这样的查询命令：“A 区一个小时后有多少头猪？”而传统的无线网络的查询命令是“A 结点有哪些数据？”。这使得传统的点对点通信模式和基于整体识别的模式在这里不再适用，而以数据为中心，根据位置信息传播的方式更适合无线传感器网络。基于位置的路由摒弃了传统基于 IP 的通信，采用基于结点的位置信息通信模式，这在传感器网络中是有效的。基于位置的路由不是简单意义的分组路由，它需要单播路由和多播路由/泛洪路由组合。基于位置的路由是基于位置信息的协议的基本组成部分。

基于位置信息的路由算法的目的是实现查询传送和广域数据提取，它与物理介质和链路选择无关，每一个基于位置的路由协议其主要目的都在于解决以下问题：

（1）结点定位

基于位置的路由是在基于结点的位置信息的基础上，每个结点只需要知道在它们的一跳或两跳距离内相邻结点的位置信息。

（2）贪婪转发

最简单的方式为当前结点选择目标区邻居结点作为下一跳结点，但容易遇到通信空洞使分组转发不能进行下去，也没有考虑到能耗和链路的状态。

（3）空洞绕行

如何避免和绕行通信空洞，是基于地理位置路由常见问题。不管是否采用什么贪婪转发方式，结点都选中目标区附近的邻居结点作为下一跳结点，如何有效应对洞问题是基于地理位置路由必须妥善解决的难题。

（4）目标域内转发

当路由分组到达目标区域，如何快速有效地将信息发送到该域的所有结点是基于地理位置路由需要认真解决的另一重要问题。

针对不同的应用，传感器网络可以用不同的方法组网，所以不同应用使用不同的路由方案。但一般而言，基于位置的路由协议主要包括两部分：一是位置服务，即位置搜索；另一个是分组转发策略。下面就位置服务和转发策略，分别从两个方面来介绍几种常见的协议和算法。

4.3.1　位置服务协议

对于基于位置信息的路由算法，每个结点通过 GPS 方法来获取自己当前的位置。位置服务（Location Servic）是指发送结点可以通过位置服务获得结点的位置信息，并把位置信息包含在目的结点发送的数据包中。

（1）简单位置服务协议（SLSP）

简单的位置服务协议类似先应式路由协议，使用定期广播实现结点位置信息的交换。每个结点存储位置表用于存储它知道的结点的位置信息，结点按一定的时间间隔向邻居结点广播位置信息。每一个位置信息包含有 N 个其他结点的位置信息，该位置信息以循环方式在结点的位置表中被选定。通过多个位置信息包交换，每个结点和邻居结点可以分享它们知道的其他结点的位置信息。同时每个结点还定期从邻居结点接收结点的位置信息，根据接收的位置信息包更新其位置表，以便让它保持最新的位置表。为了避免结点同时广播位置信息包而导致的冲突，每个结点广播时会有一个随机时间延迟。

（2）反应式位置服务协议（RLSP）

RLSP 类似于按需的路由协议，与 DSR 路由发现过程类似但有不同的目的。它是通过位置服务找到目标结点的位置信息，而无须维护这条路由。其基本思想是：当一个结点需要发送数据但不知道目的结点的位置，或者目的结点位置无效时，PLSP 第一次在邻居结点检测是否有目的结点位置信息，如果在一定时间内没有收到答复信息，它将在网络中泛洪包含源结点 ID、源结点位置和目的结点的位置信息的位置请求数据包来请求报文，并设置一个定时器。一个结点收到位置请求数据包，如果该结点知道结点的位置信息或者它就是目标结点，它利用位置请求数据包的反向源路由向源结点发送一个响应数据包，否则重新进行数据包广播。如果在一定时间内没有收到相应的响应数据包，则认为目的结点不能到达，同时展开新一轮的位置请求。为了避免无限循环重复转发数据包，每个包有一个序列号，使每一个结点只能转发一次同一位置请求包。

（3）基于网格的位置服务协议（GLS）

GLS（Grid Location Service）是一种主动式的分布式位置服务协议，具有较高的容错性和扩展性，适用于大规模的网络。其基本思想是每个结点在整个网络中维护多个位置服务器，这些位置服务器不是指定的，而是根据分布式选择算法选择的。经过分布式选择算法后，每一个结点在离它近的地方服务器数目较多，而在离它远的地方服务器数目少。这样一来位置服务器的数目会随着网格的阶数增加而减少。每个结点都有可能作为其他结点的位置服务器，位置服务器的结构也和普通的结点没有区别。

在 GLS 中，网络的划分是路由协议能够正确工作的基础，这也是最先需要做的工作，整个网络中的所有结点都会按照预先划分的网格确定自己所处的位置。整个网络按照一定的规则分割为网格，例如按经度纬度来进行划分，或在小范围内按照距离进行划分。整个

网络由各阶网格组成，网格的阶的定义如下：最小的网格的阶数为 1，n 阶网格是（n+1）阶网格的 1/4。

图 4-7 给出了网络网格划分的一小部分，每一个网格的大小是一个 R×R 的正方形，R 的大小根据无线传输范围而定，选择的原则就是要保证单个网格内的任意两个结点通过一跳或两跳就能到达。图中最小的网格称为 1 阶网格，4 个相邻的 1 阶网格组成一个 2 阶网格，4 个相邻的 2 阶网格组成 3 阶网格，以此类推，如图 4-7 所示。

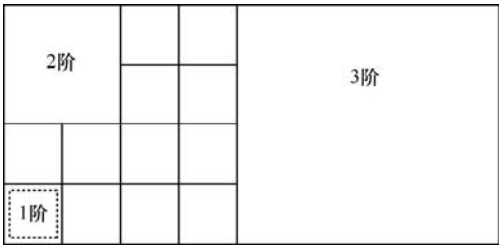


图 4-7　3 阶网格示意图

值得注意的是，并不是任意的 4 个相邻的（n−1）阶网格都能组成 n 阶网格，每个 n 阶网格最左下角的坐标必须满足 $(a\times 2^{n-1}, b\times 2^{n-1})$，其中 a，b 为整数（可以看作是一个二维平面），n=1，2，3，…同时，为了避免出现网格重叠，规定任意一个 n 阶网格能且只能属于一个（N+1）阶栅格。

GLS 的另一个突出的特点就是协议中引入了一个位置服务器的概念，每个结点把它的位置信息分别存放在网络中的多个位置服务器中，从而能够保障位置信息的快速查询。如果结点希望查询结点的位置信息，就可以通过结点的任意一个位置服务器得到结点的位置信息。此协议通过一个预先定义的很强的哈希函数把结点的唯一标识（如网络地址、MAC 地址甚至是位置信息等）映射为一个随机的识别码，称为 ID，一般为一个整数。并定义 A 的“最近结点”为大于 A 的 ID 号中最小的 ID 号所标识的结点。

图 4-8 给出了位置服务器的选择算法，结点在网格结构图中，每一阶都需要选择 3 个位置服务器，选择的策略为选取“最近结点”。各结点都维护一个位置服务器列表，其中包含了各阶位置服务器的 ID、位置和速度等。当然，其列表需要定时更新，当结点移动时也需要更新位置服务器。如图 4-8 所示，假设此时结点 S（9）开始选择它的位置服务器，那么首先在它相邻的三个等大小的网格中分别选择 23、13 和 41 作为它的一阶位置服务器，按照同样的方法选择 10、1 和 18 作为其二阶位置服务器以及 22、23 和 11 作为其 3 阶位置服务器。其中对于网格（1，4，6）由于其值均比 9 小，就选取最小的 1 作为其位置服务器，这里采取循环比较的方案，即把所有的数字排列成一个环，因此，最小也是最大。

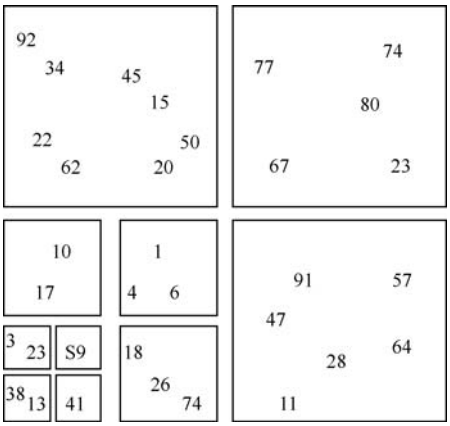


图 4-8　3 阶位置服务器选择算法示例

最终，每个结点都调用该选择算法得到自己的位置服务器，当结点需要查询其他结点的位置信息的时候，也采用类似的过程：首先在本网格内部寻找离目标结点的“最近”的结点，向它发送位置查询报文，而当这个结点收到位置查询报文后，如果它存有目标结点的位置信息，就返回一个包括目标结点位置的应答信息，否则，就从自己知道的结点中找到一个离目标结点“最近”的结点，向它转发位置请求报文，并重复此过程，直到找到目标结点的位置信息为止。

（4）虚拟极坐标系统（VPCS）

虚拟极坐标系统不需要实际的位置信息，它利用虚拟坐标代替实际坐标来进行路由的选择和数据在网络中的存储和查询。虚拟极坐标系统建立后，整个网络结点形成一个以基站或汇聚结点为根的带状树（Ringed Tree）。每个结点的虚拟坐标用两个参数表示：距离树根的跳数和角度范围。

虚拟极坐标系统的建立共分为三个阶段：生成树形结构、反馈子树的大小和确定虚拟角度范围。

生成树形结构：基站或汇聚结点进行初始化，将自己的跳数设置为 0，并广播一个路由建立消息报文，其中包括了一个到汇聚结点的跳数的域。与汇聚结点相邻的结点收到该消息后，将汇聚结点作为自己的父结点，并将自己到父结点的跳数设置为 l，然后继续广播路由建立消息，同时父结点也监听下一轮邻居结点的广播，并将发送跳数为 1 的路由建立消息的结点标记为子结点。这个过程一直扩展到整个网络，使得每一个结点都知道自己的父结点、子结点以及到汇聚结点的跳数，直到所有的结点都加入这个树形为止。其中，当一个结点收到多个广播消息的时候，选择信号最强的结点作为自己的父结点。若结点广播路由建立消息后没有收到跳数比自己更大的路由建立的消息，则认为自己是叶结点。

反馈子树的大小：树形结构建立后，从叶结点开始，结点将以自己为根结点的子树大小报告给它的父结点。其中，叶结点报告的数值为 1，中间结点的数值为所有子树大小相加再加 1。这个过程一直进行到汇聚结点，最后汇聚结点得到整棵树的大小。

确定虚拟角度范围：汇聚结点首先确定整个虚拟极坐标系统的的角度范围，如$[0,\pi]$。这个范围是一个相对的逻辑概念，根据需要可以自己定义范围。汇聚结点再将角度范围分配给每个子结点，其原则是：每个子结点得到的角度范围与以该结点为根的子树大小成正比。然后每个子结点重复同样的分配过程，最终整个树形的每个结点都得到了一个角度范围，加之前面的跳数，形成了虚拟极坐标系统。从而，可以用一个坐标（跳数、角度范围）来唯一的标识网络中每个结点的位置。

总之，只要虚拟坐标系统建立起来了，剩下的过程都是相当简单的，即便是在一个稳定的网络中建立虚拟坐标系，开销也是可以接收的。这种坐标系的一个典型的应用就是嵌入子图路由选择（GEM）。

（5）边界定位服务（GRWLI 中的位置服务过程）

在无线传感器网络的实际应用中，要让每个结点都知道自己的精确位置信息就需要花费很大的代价，而 GRWLI 中的位置服务过程的主要思想就是通过网络中已知自己位置信息的结点（信标结点）确定一个全局的坐标系，然后再确定其他结点在这个坐标系的位置。根据信标结点的选取方法的不同，GRWLI 中的位置服务过程又分为以下三种策略。

1）所有边界结点均为信标结点。

将网络实际边界上的结点均设为信标结点，在平面的情况下，结点的位置是通过邻居结点位置的平均值来计算的，如式（4-1）所示。

$$x_i = \frac{\sum_{k \in \text{neighbor_set}(i)} x_k}{\text{size_of}(\text{neighbor_set}(i))}$$
$$y_i = \frac{\sum_{k \in \text{neighbor_set}(i)} y_k}{\text{size_of}(\text{neighbor_set}(i))} \quad (4\text{-}1)$$

每个结点位置坐标的确定是个逐步求精的迭代过程：初始化阶段，将每个非边界结点的坐标值均设为（0，0）；迭代阶段，非边界结点按照式（4-1）来计算自己的坐标，每次计算后，邻居结点之间都需要相互交换新计算出的坐标值，再进行下一步的迭代。迭代结束的条件可以通过设置迭代次数或迭代停止的阈值来控制，例如设置经过 1000 次计算便停止迭代过程或者坐标变化不超过 0.05%时便停止迭代等。

2）只有两个信标结点。

这个方案要求所有的边界结点均知道自己为边界结点，但不知道自己的位置信息，其基本思想是：首先边界结点通过交换 HELLO 报文信息（主要是跳数信息）建立全局坐标

系，然后引入两个信标结点以减小全局坐标系所带来的误差。方法是通过不断地计算两个信标结点和所有的边界结点的重心坐标，然后利用计算出的重心坐标和两个信标结点重新建立全局坐标系，最后按照策略 1 的方法计算非边界结点在全局坐标系的位置。

3）只有一个信标结点。

其基本过程为：首先用这个信标结点向全网广播包含跳数字段的 HELLO 消息，中间结点将接收消息的跳数加 1 后转发，然后邻居结点交换它们各自到信标结点的跳数距离。如果一个结点到信标结点的跳数距离在两跳邻居范围内最大，则标记自身为边界结点。最后，采用和策略 2 类似的方法建立全局坐标系，并最终求得所有结点在全局坐标系中的位置。

4.3.2　几种典型的位置路由算法

分组转发策略是指结点向目的结点发送数据时如何选择下一跳。将数据发送给邻近一跳邻居结点，再由其采取同样的策略转发，最后到达目的结点。根据所采用的转发策略的不同，可以把基于位置的路由协议分为位置辅助路由算法和位置信息路由算法两类。其中位置信息路由协议又可以分为基于受限泛洪、基于贪婪转发、基于贪婪转发和能耗均衡性相结合三种方案，如图 4-9 所示。下面分别介绍这几种典型的位置路由算法。

（1）位置辅助路自（LAR）

LAR（Location Aided Routing）之所以被称作位置辅助路由，是因为它并没有提出一个基于位置信息的路由协议，而是利用目的结点的位置信息来限制路由发现过程中分组的泛洪范围，从而提高路由请求的效率。

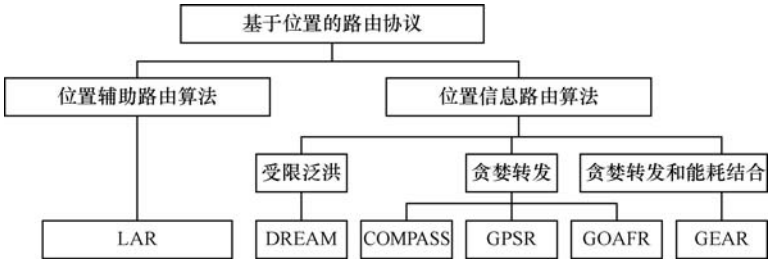


图 4-9　基于位置的路由协议分类

LAR 协议中的路由发现采用了一种类似于 DSR 和 AODV 路由协议中的泛洪方法，即源结点将路由请求信息发给它的所有邻居结点，中继结点收到路由请求信息后，先判断自己是否是目的结点。如果不是目的结点，且是第一次收到这个信息包，则将信息转发给它所有的邻结点；如果是目的结点，则将路由信息原路返回给源结点。算法中每次路由寻址，网络中每个可达结点都会至少收到一次路由请求信息包，因此网络开销较大，同时也增大

了网络拥塞的可能性。LAR 利用结点的地理位置信息减少网络中参与路由的结点数。它引入了一个期望区域（Expected Zone）和一个请求区域（Request Zone）的概念，期望区域和请求区域通过计算得出。如图 4-10 所示，期望区域的计算方法为：以目的结点在 t_0 时刻的位置为圆心，以（t_1–t_0）v 为半径的圆，其中 t_0 是对源结点而言上一个目的结点的位置确定的时刻，t_1 是当前时刻，v 是目的结点移动的平均速度或最大速度。请求区域是根据源结点位置和期望区域计算的，路由寻址限定在请求区域内，只有在请求区域内的结点才有参与路由的权限。如果在请求区域内寻址不成功，则退化到泛洪算法。请求区域的计算有两种方案，方案一中，请求区域是由源结点和期望区域确定的平行于经线或纬线的最小矩形，如图 4-10（1）所示。各结点可以通过位置信息判断自己是否处于请求区域中。当结点处于请求区域中时，收到分组后进行转发；而当结点处于请求区域之外时，收到分组后丢弃。方案二中，通过发送结点到目的结点的距离来限制参与路由的结点。如图 4-10（2）所示，源结点 S 到目的结点 T 的距离为 $DIST_S$，如果结点 A 到目的结点的距离 $DIST_A$ 满足 α（$DIST_S$）+ $\beta \geqslant DIST_A$（α和β为待定参数，视网络性能而定），则结点 A 包含在请求区域内，参与路由寻址和转发，否则丢弃分组，不参与路由寻址和转发。

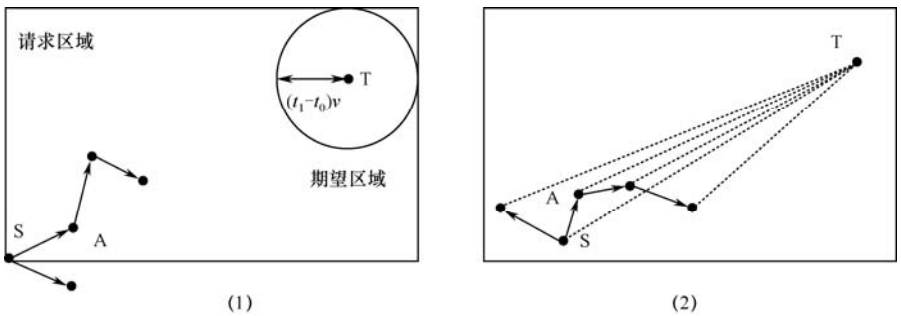


图 4-10　LAR 的请求区域和期望区域

但 LAR 路由协议也存在问题，源结点只有收到目的结点的路由回复包后才能得到目的结点的位置信息。当源端结点进行路出请求时，如果没有目的结点位置信息，则按传统广播方式进行，使得路由请求开销较大。针对这个问题，出现 ELAR1 算法。在 ELAR1 路由协议中，每个路由请求包都携带相应的中间转发结点的当前位置信息，任何一个结点收到这个请求包后，都把包内包含的其他的结点位置信息记录到自己的位置缓存表。当结点作为源端初始化路由请求时，首先查找自己位置缓存表内是否存在目的结点的位置信息，若没有，才按照 LAR 协议发送请求包。

（2）距离效应路由算法（DREAM）

DREAM（Distance Routing Effect Algorithm）是一种典型的定向区域泛洪路由协议，该协议中假设每个结点都通过 GPS 获得自己的位置信息，并以坐标的形式给出。每一个结点

都维护一个位置列表，表项内容包括每一个结点的位置信息，对应结点的方向及距离，最后是更新时间。其中，相对方向和距离可以通过计算得到。相对方向是指以结点 S 为中心建立极坐标，结点 T 的角度为γ，如图 3-5 所示，距离是指结点 S 到 T 的地理距离。每一个结点周期性地广播一个控制分组，通过控制分组进行位置更新，此分组包括结点的坐标信息和一个生存时间。大多数分组只有一个较短的生存时间，这些分组以较高的频率发送，而且在传播较短的距离后失效；而另外一些分组则拥有较长的生存时间，它们的发送频率较低，能够传送到网络中距离较远的结点。当一个结点收到控制分组，结点通过计算该分组传播的距离与生存时间比较的结果来判断是否继续转发分组，如果传播的距离大于生存时间则不再进行转发。

图 4-11 中，结点 S 在 t_1 时刻向结点 T 发送分组，S 首先在位置列表中查询结点 T 的位置信息，得到结点 T 的位置坐标，即相对于结点 S 的距离和角度，以及表项的最后更新时间。由于结点的移动性，在 t_1 时刻结点 S 并不知道结点 T 的确切位置，因此根据结点 T 的速度 v 估算出结点的位置处于圆 C 内，圆 C 的半径 x 通过（t_1–t_0）v 得到。由此可以得到一个由结点 S 进行分组转发的区域 F，将 F 定义为$[\gamma-\alpha,\gamma+\alpha]$，称为期望区域。结点 S 向这个区域内的其他所有结点进行分组转发，当其他结点收到分组后重复上面的步骤，直到结点 T 收到分组。

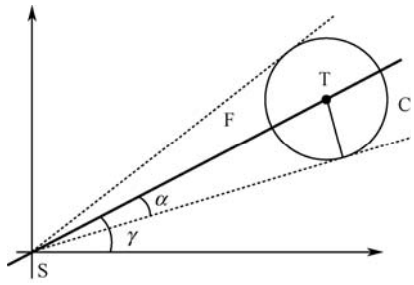


图 4-11　DREAM 分组转发示意图

DREAM 算法能保证无环路由，具有较好的鲁棒性。每次数据分组转发都是发送给目标结点方向的多个结点，类似于提供了到目标结点的多条路径，某条链路分组的丢弃不会影响到其他链路上的分组。相对于位置辅助路由算法 LAR，DREAM 算法控制分组中只有位置更新分组和 ACK 分组，携带信息更少，并且位置更新分组发布的周期根据结点的移动速度确定，在控制分组的数目和传播范围方面均得到了进一步优化，减少了大量开销。虽然限制了到目标结点的泛洪范围，但在结点数目多、数据量大的密集型网络中，数据分组在转发区域内进行泛洪仍会消耗大量的能量。

（3）贪婪周界无状态路由（GPSR）

GPSR 是由哈佛大学的 B. KARP 和 H. T. Kung 提出的基于位置路由的典型协议。与常

规的路由协议不同的是，它是利用结点的位置信息转发数据包的。运行此协议的结点不需要获得和保存整个网络的拓扑，这大大降低了对结点存储空间的要求。GPSR 协议结合了贪婪转发与边界转发的优点，而且算法较为简单，易于实现，因而成为目前无线传感器网络和移动 AD Hoe 网络中使用最广泛的基于地理位置的路由协议之一。与传统的路由协议相比，其路由开销和分组成功传输率都有较大提高。

GPSR 是一种典型的基于传统贪婪转发方案的路由协议。为了避免传统贪婪转发方案中通信空洞造成的路由寻径失败，以及由此产生的重复路由请求带来的额外开销，GPSR 利用传感结点对位置信息的可知性和结点处于相对静止状态的特点，在路由过程遭遇通信空洞而失效时根据网络原始拓扑，生成一个平面子图，并沿子图中空洞的周界进行分组转发。同时 GPSR 算法还利用该机制来支持传感结点的移动性。GPSR 协议建立在传统贪婪转发算法之上，具有贪婪转发和周界转发两种分组转发方式。路由开始时采用贪婪转发方式进行分组转发，当贪婪方式失效时（即遇到通信空洞时）转入周界转发模式继续路由，一旦条件满足时恢复贪婪转发模式，如此反复直至分组到达目的地。

1）贪婪转发模式。

贪婪转发算法是一种基于位置信息的路由算法。贪婪转发算法的前提是每个分组都已包含其目的结点位置或目标区域位置，每个结点都知道自己和直接邻结点的位置。贪婪转发算法的选择策略一般是在发射半径内向最远处转发（Most Forward Within R：MFR），即向着信宿方向的最远的邻居结点为下一跳，向处在发射半径内离目标结点或目标区域距离最近的结点转发。当然，根据实际情况和网络状况，还可以选择信宿方向的最近转发（NFR）和最接近信源到信宿的直线转发（CSL）等转发策略。当出现路由空洞，即不存在满足贪婪转发条件的邻接点时，算法进入周界转发模式。

2）周界转发模式。

算法按照右手定则转发分组至其逆时针方向结点，直到分组到达某结点 X，其中当结点 X 与目的地位置的距离小于进入周界转发模式时结点与目的位置的距离时，算法将在结源点点 X 上转为贪婪转发模式。

图 4-12 描述了一个数据分组采用 GPSR 算法从源点 S 转发到目标结点 D 的过程。首先根据贪婪转发的最远转发原则，源点 S 将数据分组按照箭头所示的方向依次转发至结点 A。由于结点 A 找不到比自己离目的结点更近的结点（结点 A 的两个邻居结点都比自身离 D 更远，即 A 局部极小点），结点 A 进入周界转发模式。在周界转发模式下，结点 A 按照右手定则将数据分组依次转发给结点 X，结点 X 发现到目标结点 D 的距离已经小于到 A 的距离，此时结点退出周界转发模式，在 X 处回到贪婪转发模式进行转发，最终用贪婪转发到达目的结点 D，完成此次转发。

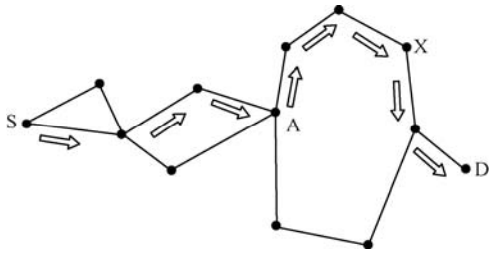


图 4-12　GPSR 算法转发示例

有很多协议都是基于这个思路的，具有代表性的如第二代指南针路由算法和 DOAFR 算法等。其中第二代指南针路由（Compass Routing II）是最早能确保到达目标的位置路由，和 GPSR 不同的是，它是一个不包括贪婪转发模式的纯表面路由算法，没有采用右手定则的方法遍历表面，而是利用源目结点连线和表面的交点来切换不同的表面，最终切换到目标结点所在的表面完成转发。由于不含贪婪转发，因此收敛速度较慢，效率较低。而 GOAFR 是在 GPSR 基础上进行改进的路由算法，它引入了一个椭圆边界来防止在某些情况下（如路由空洞面积极大）算法性能的急剧恶化。此外，其表面切换的触发条件也进行了改进，由原来单一的源目结点连线变成每个表面入口结点和目标结点的连线，这种带有自适应的切换方式加快了算法的收敛速度，同时椭圆边界的引入也保证了算法在最坏情况下具备最优的复杂度。

（4）位置和能量参照路由（GEAR）

GEAR（Geographical and Energy Aware Routing）能源有效性，是一个基于贪婪转发与结点能耗均衡性相结合方案的路由协议。GEAR 算法中，传感器网络中的数据包含了位置属性信息，利用这一信息，把在整个网络中扩散的信息传送到适当的位置区域中。同样 GEAR 也采用了查询驱动数据传送模式。它传送数据分组到目标域中目的结点的过程包括两个阶段：向目标域传送数据和域内数据转发。在向目标域传送数据阶段，在选择邻结点进行下一跳转发的同时，把各直接邻结点的能量信息结合起来考虑，选择综合开销最小的邻结点进行分组转发。基于贪婪转发与结点能耗均衡性相结合方案的路由算法中，综合开销最小的邻结点的选择至关重要。

1）向目标域传送数据阶段。

GEAR 根据邻结点通往目的地的已知代价（Learned cost）来确定下一跳结点，使得分组能够朝向目的地转发，同时还可以平衡邻结点的能量消耗。GEAR 算法的关键是建立和维护结点的已知代价 L（N，R）。假设结点 N 准备转发分组 P，其目的地是 R，而且 R 的中心点是 D。结点 N 既要把分组往目标区域转发，同时还要尽量平衡其所有邻结点的能量消耗，结点 N 通过使邻结点 N_i 的 L（N_i，R）最小来实现这种折中。如果结点 N 的缓存中没有关于 N_i 的 L（N_i，R），则使用估计代价（estimated cost），即 c（N_i，R）作为 L（N_i，R）的缺省值。估计代价 c（N_i，R）的定义如下：

$$c(N_i,R)=a\times b(N_i,R)+(1-a)\times e(N_i) \tag{4-2}$$

其中 a 是可调权值，d（N_i，R）是把 N_i 到 D 的距离与 N 的邻结点中距离 D 最远的长度相比得出的值，e（N_i）是把 N_i 消耗的能量与 N 的邻结点中已消耗的最大能量进行比较得出的值，因此，d（N_i，R）和 e（N_i）都是归一化后的参数值。在 N 选择了具有最小综合开销的邻结点 N_{min}。作为下一跳结点后，结点 N 就把自己的 L（N，R）设置为 L（N_{min}，R）+c（N，N_{min}），其中 c（N，N_{min}）是从 N 传送一个分组到 N_{min} 所需开销。通过这样的一种策略不断地调整已知代价，当第一个分组到达目的地时，正确的 learned cost 值就会被往后传输一跳距离。每当一个分组被转发时，正确的 learned cost 值都会被传播给一跳范围内的结点，使得每次转发后都将正确的综合开销值在一跳范围内进行回传，以便结点下一次转发目的地相同的分组时直接选择正确的邻结点，减少额外的开销。

在向目标域传送数据过程中，有两种情况要考虑：一种是存在距离目的地更近的邻结点，GEAR 则只从这些邻结点中选择距离目的地更近而且已知代价最小的结点作为下一跳；另一种是不存在距离目的地更近的邻结点，即遇到路由空洞，GEAR 就从所有的邻接点中选择一个可以使得该邻结点的已知代价最小的结点作为下一跳。

2）域内数据转发阶段。

当分组被转发进入目标区域后，大多数情况下采用递归的、基于位置信息的转发方式在目标区域内转发分组。如图 4-13 所示，假设大矩形就是目标区域，当路由分组转发到了位于目标区域内的 N_i 结点时，N_i 发现自己就在目标区域内，于是把目标区域分成四个小矩形子区域（分别位于目标域的 I、II、III、Ⅳ象限），并把分组向这四个子目标区域进行转发，在向子区域转发分组的时候同样遵循自定面所讲的规则。重复这个区域划分和转发的过程，一直到结点发现自己是某个子区域内唯一的结点，或者某个子区域没有结点存在的时候，这个子区域结束转发。当所有子区域转发过程全部结束时，整个迭代过程终止。

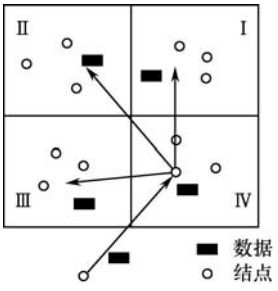


图 4-13　GEAR 目标区区域数据递归转发

然而在一些结点密度低的情况下，这种递归的转发方式有时可能进入死循环，无法停止下来，会围绕着一个空目标区域进行无用的路由，除非分组的跳数记录（hop-count）超

过了给定阈值。这种情况下可采用受限洪泛的方式进行分组转发，但当结点密度较大时，这种方式的开销比较大。洪泛机制和迭代机制各有利弊，GEAR 采用如下方法来选择域内转发机制：当查询命令到达域内的第一个结点时，如果该结点的邻居数量大于一个预设的阈值，就采用递归转发机制，否则使用洪泛机制。

4.4 无线传输路由与常用协议

Ad hoc 网络是由无线移动结点构成的自组织网络，没有类似基站、路由器的静态网络结构，所有结点都可以随机地、自由地移动，其网络拓扑结构是动态变化的。在 Ad hoc 网络中只有相邻结点之间才能进行通信，若两个结点之间的距离超出传输范围（一般为 150～250m），那么必须通过一个或多个中间结点以“多跳”的方式来转发信息，因此 Ad hoc 网络的关键问题之一是设计有效的、自适应的路由协议，保证任意两个移动结点在网络拓扑变化以后仍能实现高质量的通信。Ad hoc 网络在军事、紧急救助和探险等领域具有非常重要的应用前景。

传统的路由算法主要基于距离矢量（distance vector）或链路状态（Link state）。距离矢量路由中，每个结点维持所有可能到达结点的距离矢量表，并向周围结点周期性地广播自己的路由表，同时根据相邻路由表接收到的值来计算自身路由表的更新值。通过比较到每一个相邻结点的距离，路由器可以确定将哪个结点作为它的“下一跳”（next hop），以便于具有最短路径。链路状态路由中，每个路由表维持一个完整的全网拓扑图。每个结点管理到相邻结点链路的损耗，并周期性地广播更新的链路信息。根据每一条链路的信息，每个结点路由表计算到所有可能的目的端的最短路径。由于这两种路由算法所消耗的 CPU 时间负荷和网络带宽都比较大，因此不能直接应用于 Ad hoc 网络。

Ad hoc 网络中的移动结点使用电池供电，结点之间的无线干扰严重限制了网络吞吐量，结点的移动性难以管理，因此在路由算法的设计中应主要解决减少能量消耗、减小延迟、提高吞吐量等问题。

现存 Ad hoc 网络路由协议可以分为两类：表驱动（table-driven）和源发起按需驱动（source-initiated on-demand routing）。

4.4.1 表驱动路由协议

表驱动路由协议（table-driven routing protocols）是有线网络路由协议向 Ad hoc 网络的移植。网络中的每个结点维持一个或多个表格来存储其他结点的路由信息，通过广播更新信息来保持路由表信息与网络拓扑的变化之间的一致性。典型的表驱动路由协议包括：

DSDV（destination-sequenced distance-vector routing）、CGSR（cluster head gateway switch routing）和 WRP（wireless routing protocol）等。

（1）DSDV 协议

DSDV 协议是先应式路由协议，是由传统的 Bellman-Ford 路由协议改进得到的，其特点是利用目的结点序列号解决了 DBF 算法中的路由环路和计数至无穷问题。

DSDV 要求每个结点保存路由表，表中列出了所有可达的目的结点及到达该目的结点的跳数。每个路由条目包含目的结点产生的序列号，用来区分新旧路由。结点间通过周期性地发布路由更新分组来交互路由信息，以保证路由表的正确性。当有重要的新信息是由广播路由更新分组。移动结点收到新的路由信息分组时，路由的更新遵循以下两个原则：比较该更新分组中携带的路由信息和结点保存的路由条目。如果结点收到的路由的目的结点序列号大于路由表中相应的目的结点的序列号，则采用有更新序列号的路由而丢弃原有的旧序列号的路由；如果更新分组中目的结点序列号与现存的序列号相同，则选择具有较好度量的路由条目，若新路由有较好度量，则丢弃现存的路由或将其存储为次之路由。

为了减轻网络的负担，路由更新分组采用两种形式：一种为“full dump”，它携带结点所有的路由表信息；另一种为“增长”（Incremental）型数据分组，它携带的信息是自上次发送 full dump 以后结点的路由表中发生变化的那些路由条目的信息。移动结点还保存一个附加表来存储已经在增长型路由信息数据内传送的数据。

当网络中拓扑结构改变时，DSDV 算法采用以下两种方法来检测链路的中断：

链路层检测到某条链路中断时，向路由层报告。检测是通过时间来推断，即结点在过了一段时间后仍没有收到某个结点发送的分组，就自动认为本结点到该结点的链路中断，将相应的路由条目设置为无穷大（实际中，若链路度量为跳数，则经常设置为 N+1，N 为网络的结点数）来描述断开的链路。

检测出链路中断的结点会发送一个更新分组，该分组有一个新的序列号，跳数为无穷大。这会引起网络中路由表的更新，只有当再次收到丢失结点的信息后新的路由才会重新建立起来。

虽然在网络拓扑变化频繁的情况下，DSDV 协议的收敛性能不好，但在一般情况下，其收敛还是相当快的。但是，当加入网络的结点越来越多，路由表容量及开销和带宽也相应的增加。结点不一定用到连通所有目的结点的路由条目，多余的路由条目也会造成资源的浪费。DSDV 协议仅支持双向链路，也就限制了其在无线网络中的使用。最后，当结点的移动率较高时，DSDV 协议的性能将急剧恶化。

（2）WRP 协议

在 WRP 协议中，结点保存的信息表包括距离表、路由表、链路开销表、分组重传列表 4 个部分。结点通过获得邻结点的状态变化信息来维护自己的信息表，并通知邻结点。收到

来自邻结点的信息后，要更改保存的信息表，结点需要发送一个回复分组（ACK）用来说明已经收到并处理了某个更新消息。若结点没有转发数据分组或更新消息，则要定期发送 HELLO 分组，以确保结点间的连通性。结点在一段时间内没收到邻结点发送的任何分组，就认为和该邻结点间的链路失败。结点就要重新计算到受影响的目的结点的距离和对应的前驱结点，并且向其邻结点发送更新分组，通知哪些目的结点的距离和前驱结点发生变化。

由于有先驱结点的记录，该协议可以有效地避免路由环路。WRP 要求结点维护 4 张路由表，这会给结点带来负担，特别是结点较多的时候。由于利用 HELLO 分组保持连通性，WRP 不允许结点处于睡眠状态，这会耗费电池电量，同时网络的带宽也会被更新分组大量占用。

（3）OLSR 协议

OLSR 协议是对纯链路状态算法进行优化而形成的。协议的核心是多点中继，即通过减少同一区域内相同控制分组的重传转发次数来减少网络中广播分组的数量。网络中的每一个结点选取其邻结点的一个子集用于转发该结点发送的控制分组。这些被选择的结点就成为该结点的 MPR，而该结点就成为这些 MPR 的多点中继选择结点（MPR Selector）。协议根据选择的 MPR 集来计算到所有目的结点的路由。网络中的每个结点都周期地广播它的 MPR Selector 的信息，结点各自收到这一消息后，计算并更新自己到达相应目的结点的路由。因此，路由就是通过从源到目的结点的 MPR 的逐跳结点序列。

该协议适用于在使用时维护的信息较多且到新目的结点的路由请求较频繁的网络。OLSR 通过减少同一区域内相同控制分组的重复转发次数，显著减少了网络中广播分组的数量，特别适用于网络规模大、结点分布密集、结点间通信频繁的网络。同时，该协议还具有找路时延小的优点。

（4）STAR 协议

上述几种协议算法，都是遵守 ORA（Optimum Routing Approach，最佳算法）原则的，而 STAR 协议是第一个遵守 LPRA（Least-Overhead Routing Approach，最小开销算法）原则的先应式路由协议。STAR 协议建立路由后，并不试图维护最佳路由，它使用以源结点为根的路由树存储路由信息，当路径可能产生环路时主动向相应的结点发信号，不需要用周期更新来验证路径的有效性，大大降低了开销。

STAR 协议的控制开销较小，允许采用次最佳的路由。STAR 协议通过只传播通往目的结点必需的链路状态信息来减少带宽的消耗，利用这些信息来决定发更新分组的时机，检测新的目的结点、不可达目的结点和路由环路。

（5）TBRPF 协议

TBRPF 协议是一种先应式的链路状态路由协议，提供逐跳的最短路径。每个结点根据缓存在拓扑表中的局部拓扑信息，利用 Dijkstra 算法，计算到目的结点（网络中的其他结

点）的路由。TBRPF 协议包括两个模块。

路由模块：TBRPF 使用周期性的更新消息和增量的更新消息保证邻结点获得计算路由所需的状态信息——结点源树的一部分。为了减少开销，每个结点只向邻结点报告自己的部分源树——源树的报告部分。为了改善协议的鲁棒性，让结点获得更多的拓扑信息从而计算出多条路径，并且使得中继优先级高的结点尽可能地为其他结点转发分组，每个结点可以独立地选择报告除源树的报告部分之外的拓扑信息。

邻居发现模块：通过“增量 HELLO”分组，结点可以实现邻居发现功能。结点周期性发送的增量 HELLO 分组只报告发生变化的邻结点的状态信息，而不是报告所有的邻结点的状态信息，所以其分组长度比其他链路状态路由协议的分组长度要小得多。

该协议是 R.Ogier 等人在 1999 年提出的一种应用于多条网络中的广播路由协议，该协议考虑如何向网络中所有结点广播拓扑信息（包括链路费用信息和链路通/断状态信息）。此后，该协议经修改后，变成了一种有本质差别的路由协议——基于逆向路径转发的拓扑分发路由协议，又称为 TDRPF 协议。

表驱动路由协议虽然可以很快地获得其他所有结点的路由，但是不可避免地存在信号拥塞和能量过度消耗的问题，而且表驱动路由协议逐渐为需驱动路由协议所替代。

4.4.2 源发起按需路由

按需路由协议不需要像表驱动路由协议那样实时地维持每个结点的路由信息，而只在源结点需要路由的时候才发起路由，从而降低了对网络带宽和能量的过度消耗。当源结点需要一个到达某一目的结点的路由时，它在网络中发起一个路由发现过程即路由建立之后，会由一个路由维护程序进行维护，直到每条路径都断裂或不再需要路由为止。典型的源发起按需路由包括 AODV（Ad hoc on-demand vector routing）、DSR（dynamic source routing）、TORA（temporally ordered routing algorithm）等。下面会介绍有关协议。

（1）DSR 协议

DSR 协议的特别之处是它运用了源路由算法，即只有发送结点知道完整的到目的结点的多跳路由，这些路由被储存在 cache 内。被发送的数据分组在其分组头内携带源路由信息。

一个 Ad hoc 网络中的结点欲发送数据到目的结点，但是当它检查自己缓存中没有到目的结点的路由时，它将启动路由发现过程。源结点用泛洪的方式给网络中的其他结点发送路由请求分组（RREQ），每一个收到该分组的结点都向它的邻结点转发该分组，除非它就是目的结点或者在它的 cache 中存有到目的结点的有效路由。这样的结点将会回复一个路由应答分组（RREP）给源结点。RREQ 和 RREP 分组也是服从源路由算法的。由 RREQ 分组建立了一条到目的结点的穿越网络的路径，RREP 分组利用该路径反转路由回到源结点。

源结点则将收到的 RREP 分组所携带的路由信息并储存到它的 cache 内以备后用。

如果源路由中的任何一段链路由于一些原因中断了，则会有一个路由出错分组（RRER）通知源结点。源结点会将它的 cache 内的包含那一跳的路由删除，并且源结点将会启动新的路由建立过程。协议作者还提出了一些优化措施来使协议更有效，优化措施如下所述。

抢修：当分组传送过程遇到链路断开时可由中间结点根据自己的 cache 来选择另一条路由。在发送 RERR 分组之后，结点可能试图抢修遇到路由出错的数据分组而不是丢弃它。结点首先搜索自己的路由缓存，若查找到到目的结点的路由，则通过用自己缓存中的路由替换分组中的源路由来抢修数据分组。

无确认路由修复：源结点在收到 RERR 分组时，可把它包含在下次发送的 RREQ 中，这样可以帮助网络中其他结点获得 RERR 信息，刷新 cache。

混合侦听：当结点侦听到并不是发给自己的分组时，它检查存储器，如果有通过自己的更好的路由，就发送 RREP 给源结点。这样可以让结点不需要直接参与路由过程就获得路由信息。另外，如果听到的是 RREP 分组，对方就停止 RREP 的传送，可以在一定程度上避免 RREP 分组泛滥。

随机延迟：为了防止 RREQ 在泛洪过程产生冲突，每个结点在转发收到的 RREQ 分组前将随机延迟一段时间。结点可以为某个路由请求启动路由建立过程，但在收到 RREP 分组之前，如果还没有超过最小时间限制，则结点不为该请求再次启动路由建立。

路由建立过程稍带数据分组：在业务产生而结点没有路由可用时，启动路由建立机制。在等待路由应答的这段时间内，数据分组或者被缓存或者被丢弃。如果在 RREQ 中捎带数据分组，可以从一定程度上减少分组传输的时延，但是数据分组不能太大。当然，如果中间结点收到路由请求分组并根据它的路由缓存发送分组，就会丢弃捎带的数据分组。为了避免这种情况，中间结点在丢弃 RREP 分组之前，必须重新构造数据分组。而且数据分组的路由分为两段：前一段来自 RREQ 分组的路由记录部分，后一段来自路由缓存，而且该数据分组的源结点为启动路由建立的结点。

（2）AODV 协议

同 DSR 协议一样，AODV 协议也是一种按需路由协议，它根据业务需求建立和维护路由。AODV 协议是由 DSDV 协议算法发展而来，它应用传统的路由表。AODV 路由协议的路由发现和维护过程与 DSR 路由类似，不同的是 AODV 路由协议中，路由中的每个结点都必须维护路由表。AODV 在每个中间结点中隐式保存了路由请求和回答的结果，而 DSR 将结果显式保存在路由请求和路由回答分组中。AODV 路由的分组无须包含完整的路径信息，它采用逐跳转发的方式，从而减小了分组开销。

为了找到通往目的结点的路由，源结点将广播一个 RREQ 分组，收到 RREQ 分组的中间结点根据 RREQ 中的信息，建立到源结点的路由，称为“反向路由”。反向路由条目的

目的结点是广播 RREQ 的源结点，下一跳结点是将 RREQ 发送给本结点的邻结点，然后它向周围结点广播次分组。如果目的结点收到 RREQ 则向源结点回复 RREP。RREP 沿着刚建立的反向路由向源结点传送，在此过程中，收到 RREP 结点建立的到目的结点的路由，称为“正向路由”。正向路由条目的目的结点是 RREP 分组的源结点，下一跳是将 RREP 发送给本结点的邻结点。路由协议只维护那些正在使用的路由，而不在激活路由上的结点的移动并不影响该路由。AODV 协议设计了两种路由维护方式：源结点路由重建和本地修复。

AODV 协议的一个重要特征是在每个结点中的每个路由条目都包含了一个计时器，如果一段时间内一条路由条目没有使用，则路由条目过期。AODV 协议是 DSDV 协议和 DSR 协议的结合，它使用 DSDV 协议中的目的结点序列号防止缓存的路由信息过期以及环路的产生，路由建立是基于 DSR 协议所采用的方法，不同点在于 AODV 协议是逐跳路由而不是源路由。

（3）ABR 协议

ABR 协议是从路由的有效时间的角度来设计，选择路由的标准是路径有效时间的长短（稳定性）而不是路径长短。

该协议由以下 3 个部分组成：路由建立阶段、路由重建阶段和路由删除阶段。它明确提出使用邻结点空间、时间、连接和功率特点来构建一条生存时间长的路由。如果在下一时刻由于结点的移动或电量缺乏而使路径中断，那么即使路由条数少也没有太大意义。因此，在自组网中，应当要求路由可以持续较长一段时间，最好持续到一个连接结束。另外，ABR 协议是源始发协议，意味着不需要周期的路由更新，也不需等待路由收敛，自然地克服了表驱动协议的暂时环路现象。ABR 协议不使用路由缓存，因为维护这些缓存信息的有效性将占用大量的控制开销。

（4）TORA 协议

TORA 协议是基于“逆向链路”算法的路由协议，是具有高度的自适应性的分布式路由算法。它既不是距离矢量路由算法，也不是链路状态路由算法。它能提供原结点到目的结点的多条路由，当拓扑发生变化时，它可以把控制信息限制在拓扑变化点的一个很小范围内，从而降低开销。

TORA 协议具有 3 个阶段：路由建立阶段、路由维护阶段和路由消除阶段。路由建立和维护采用“高度”作为度量标准来建立有向无回图（DAG），路由创建由 QRY（查询）和 UPD（更新）两个控制分组完成。路由维护是在结点检测到链路失败时，采用部分链路翻转算法，保证路由正确维护以目的结点为根的 DAG 的过程。在路由清除过程中结点广播 CLR 命令，清除无效路由。该算法的缺点在于会产生类似于距离矢量算法中计数到无穷的问题，会在网络中产生振荡的隐患。

4.5　ZigBee、Wi-Fi 与蓝牙技术

4.5.1　ZigBee

1. ZigBee 简介

基于 IEEE 802.15.4 标准的 ZigBee 技术是一种近距离、低复杂度、低功耗、低数据速率、低成本的无线通信技术，是目前无线传感器网络的首选技术之一。其开发是为了建立一种低成本、低功耗的小区域无线通信方式，在此基础上通过软件协议栈发展出易布建的不依赖现有通信网络和现有电力网络的大容量无线网络。ZigBee 技术主要适用于自动控制和远程控制领域，可以嵌入各种设备。在工业控制、家庭智能化、无线传感器网络等领域有广泛的应用前景。

从应用技术来说 ZigBee 是 IEEE 802.15.4 协议的代名词。根据这个协议规定的技术是一种短距离、低功耗的无线通信技术。这一名称来源于蜜蜂的 8 字舞，由于蜜蜂（Bee）是靠飞翔和“嗡嗡”（Zig）地抖动翅膀的“舞蹈”来与同伴传递花粉所在方位信息，也就是说蜜蜂依靠这样的方式构成了群体中的通信网络。

ZigBee 联盟是一个非牟利行业组织，成员包括国际著名半导体生产商、技术提供者、代工生产商以及最终使用者。成员正制定一个基于 IEEE 802.15.4 协议且可靠、性价比高、功耗低的网络应用规格。目前已有超过 150 多家成员公司正积极进行 ZigBee 规格的制定工作。其中包括 7 位推广委员、半导体生产商、无线技术供应商及代工生产商。ZigBee 联盟的主要目标是通过加入无线网络功能，为消费者提供更富弹性、更易用的电子产品。ZigBee 技术能融入各类电子产品，应用范围横跨全球民用、商用、公用及工业用等市场。生产商最终可以利用 ZigBee 这个标准化无线网络平台设计简单、可靠、便宜又省电的各种电子产品。ZigBee 联盟的焦点在于制定网络安全和应用软件层，提供不同产品的协调性及互通性测试规格，在世界各地推广 ZigBee 品牌并争取市场的关注，管理技术的发展。

2. ZigBee 体系结构分析

ZigBee 是一组基于 IEEE 802.15.4 无线标准研制开发的，有关组网、安全和应用软件方面的技术。IEEE 802.15.4 仅处理 MAC 层和物理层协议，ZigBee 联盟定义了网络层、安全层、应用层以及各种应用产品的资料，对 API 进行了标准化。

（1）ZigBee 协议结构

相对于其他无线通信标准，ZigBee 协议结构显得更为紧凑和简单。图 4-14 为 ZigBee 协议的体系结构，大致分为底层硬件模块、中间协议层和高端应用层三部分。

<table>
<tr><td colspan="2">用户应用程序</td><td rowspan="4">高端应用层</td></tr>
<tr><td colspan="2">应用层（APL）（高级管理功能）</td></tr>
<tr><td>设备配置（ZDC）子层</td><td>设备对象（ZDO）子层</td></tr>
<tr><td colspan="2">应用支持（APS）子层（提供 ZigBee 端点接口）</td></tr>
<tr><td colspan="2">网络层（建立和维护网络连接）</td><td rowspan="4">中间协议层</td></tr>
<tr><td rowspan="2">IEEE 802.15.4 LLC</td><td>IEEE 802.2 LLC</td></tr>
<tr><td>SSCS</td></tr>
<tr><td colspan="2">IEEE 802.15.4 MAC（设备间数据传输）</td></tr>
<tr><td>IEEE 802.15.4
868/915MHz PHY</td><td>IEEE 802.15.4
2.4GHz PHY</td><td rowspan="2">底层硬件模块</td></tr>
<tr><td>底层控制模块</td><td>RF 收发器</td></tr>
</table>

图 4-14　ZigBee 体系结构层次框图

1）底层硬件模块

底层硬件模块是 ZigBee 技术的核心模块，所有嵌入 ZigBee 技术的设备都必须包括底层硬件模块。它主要由射频 RF（Radio Frequency）、ZigBee 无线 RF 收发器和底层控制模块组成。

底层控制模块定义了物理无线信道和 MAC 子层之间的接口，提供物理层数据服务和物理层管理服务。物理层数据服务从无线物理信道上收发数据；物理层管理服务维护一个由物理层相关数据组成的数据库。数据服务主要包括：

① 信道能量检测：为网络层提供信道选择依据。它主要测量目标信道中接收信号的功率强度，检测结果为有效信号功率和噪声信号功率之和。

② 链路质量指示：为 MAC 层或者应用层提供接收数据帧时无线信号的强度和质量信息。对信号进行解码，生成一个信噪比指标。这个信噪比指标和物理层数据单元一起提交给上层处理。

③ 空闲信道评估：判断信道是否空闲。ZigBee 协议标准定义了三种空闲信道评估模式。第一种是判断信道的信号能量，若信号能量低于某一个门限量，则认为信道空闲；第二种是判断无线信道的特征，这个特征主要包括两方面，即扩频信号和载波频率；第三种其实是前两种模式的综合，同时检测信号强度和信号特征，给出信道空闲判断。

2）中间协议层

中间协议层由 IEEE 802.15.4MAC 子层、IEEE 802.15.4 链路控制（Logical Link Control，LLC）子层、网络层 NWK 以及通过业务相关聚合子层 SSCS（Service Specific Convergenc sublayer）协试承载的 IEEE 802.2 LLC 子层（选用）组成。

① MAC 子层：使用物理层提供的服务实现设备之间的数据帧传输。LLC 子层在 MAC

子层基础上，在设备间提供面向连接和非连接的服务。MAC 子层提供两种服务，MAC 层数据服务和 MAC 层管理服务。前者保证 MAC 协议数据单元在物理层数据服务中的正确收发；后者维护一个存储 MAC 子层协议状态相关的数据库。

② NWK 层：负责建立和维护网络连接，独立处理传入数据请求、关联、解除关联和孤立通知请求。

③ SSCS 和 IEEE 802.2 LLC：只是 ZigBee 标准协试中可能的上层协议，并不在 IEEE 802.15.4 标准的定义之内。SSCS 为 IEEE 802.15.4 的 MAC 层接入 IEEE 802.2 标准中定义的 LLC 子层提供聚合服务。LLC 子层可使用 SSCS 的服务接口访问 IEEE 802.15.4 网络，为应用层提供链路层服务。

3）高端应用层

高端应用层主要包括应用支持（APS）子层、ZigBee 设备对象（ZDO）子层、ZigBee 设备配置（ZDC）子层、应用层（APL）和用户应用程序五部分。

① APS 子层：主要提供 ZigBee 端点接口。应用程序将使用该层打开或关闭一个或多个端点，并且获取或发送数据。

② ZDO 子层。通过打开和处理目标端点接口来响应接收和处理远程设备的不同请求。与其他的端点接口不同，目标端点接口总是在启动时就被打开并假设绑定到任何发往该端口的输入数据帧。

③ ZDC 子层：提供标准的 ZigBee 配置服务，定义和处理描述符请求。远程设备可通过 ZDO 子层请求任何标准的描述符信息。当接收到这些请求时，ZDO 会调用配置对象以获取相应的描述符值。

④ APL 层：提供高级协议管理功能。

⑤ 用户应用程序：主要包括预置的应用软件。同时，为了给用户提供更广泛的应用，该层还提供了面向仪器控制、信息电器和通信设备的嵌入式 API，从而可以更广泛地实现设备与用户的应用软件间的交互。

（2）ZigBee 网络设备及拓扑结构

IEEE 802.15.4/ZigBee 协议定义了两种相互配合使用的物理设备——全功能设备和削减功能设备。

① 全功能设备（Full function device，FFD）。可支持任何一种拓扑结构，可作为网络协调器，具有转发与路由能力，拥有足够存储空间来存放路由信息，处理控制能力相应较强。

② 削减功能设备（Reduced function device，RFD）。内存小，功耗低，只支持星型结构，不能成为网络协调器和路由器，只发送与接收信号，实现简单。

在 IEEE 802.15.4 协议中，共有 14 个物理层参数，35 个媒体接入控制层基本参数。对于 FFD，要求支持所有的 49 个参数；对于 RFD，最小支持 38 个。任一 ZigBee 网络必然

存在三种功能设备——网络协调器、网络结点和 IEEE 终端结点。其中前两者为 FFD，后者为 RFD。

IEEE 802.15.4/ZigBee 协议中明确定义了三种拓扑结构：星型结构（Star）、簇状结构（Cluster tree）和网状结构（Mesh），如图 4-15 所示。

ZigBee 星型网络对资源要求最低，它不支持 ZigBee 路由器，信号被集中到一个中心接入点，中心接入点与其他子结点的无线连接质量决定了网络的可靠性。在工业应用中，可能很难为中心接入点找到一个位置来为所有在网络中的子结点提供稳定可靠的通信连接，将中心结点的位置适当移动可能会提高中心结点与某个子结点的通信质量，但这样做经常以损害中心结点与其他子结点通信质量为代价。所以，星型结构适于小范围组网。

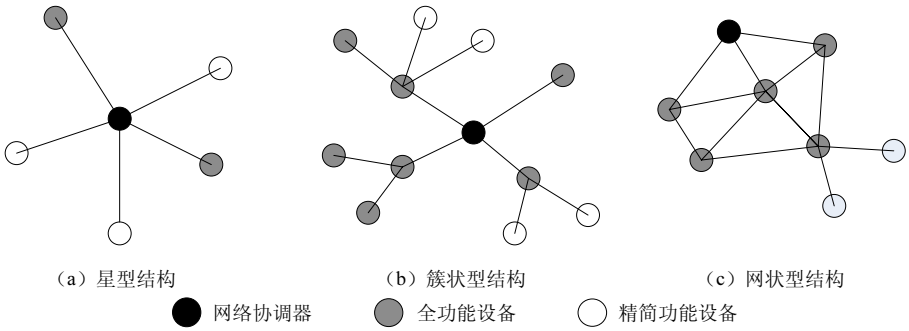


图 4-15　ZigBee 网络拓扑结构示意图

各星型网络之间通过路由结点连接构成簇状网。相对于星型网络，簇状网络覆盖的物理范围更大，容纳的网络子结点数量更多。但随着网络级联的增大，使得传输一个数据包需要的延迟更大，丢包率也随之增加。

网状结构是这三种结构中最复杂的一个。它属于 Ad hoc 多跳网络。一个网状网类似于一个簇状配置，除了 FFD 可直接将消息路由到其他 FFD 而不是遵从树结构，消息必须还是通过 RFD 的父结点到达 RFD。这种拓扑的优点在于消息反应时间缩短且可靠性提高，具有自愈性，在个别结点遭到破坏时，信息可绕过故障结点，通过其他结点传播。

3. ZigBee 无线数据传输网络

简单地说，ZigBee 是一种高可靠的无线数据传输网络，类似于 CDMA 和 GSM 网络。ZigBee 数据传输模块类似于移动网络基站。通信距离从标准的 75m 到几百米、几千米，并且支持无限扩展。ZigBee 是一个由多达 65000 个无线数据传输模块组成的无线数据传输网络平台，在整个网络范围内，每一个 ZigBee 网络数据传输模块之间可以相互通信。ZigBee 包含简单的点到点、点到多点通信（目前有很多这样的数据传输模块），包装结构比较简单，主要由同步序言、数据、循环冗余校验（CRC）几部分组成。ZigBee 采用数据帧的概念，

每个无线帧包括了大量无线包装，包含了大量时间、地址、命令、同步等信息，真正的数据信息只占很少部分，而这正是 ZigBee 可以实现网络组织管理、实现高可靠传输的关键。同时，ZigBee 采用了介质访问控制技术（MAC）和直扩序列调制技术（DSSS），能够实现高可靠、大规模网络传输。

ZigBee 定义了两种物理设备类型：全功能设备（FFD）和精简功能设备（RFD）。一般来说，FFD 支持任何拓扑结构，可以充当网络协调器，能和任何设备通信。RFD 通常只用于星形网络拓扑结构中，不能完成网络协调器功能，且只能与 FFD 通信，两个 RFD 之间不能通信。RFD 的内部电路比 FFD 少，只有很少甚至没有消耗能量的内存，因此实现相对简单，也更利于节能。在交换数据的网络中，有三种典型的设备类型：协调器、路由器和终端设备。一个 ZigBee 由一个协调器结点，若干个路由器和一些终端设备结点构成。设备类型并不会限制运行在特定设备上的应用类型。

协调器用于初始化一个 ZigBee 网络，它是网络中的第一个设备。协调器结点选择一个信道和一个网络标识符（又称 PANID），然后启动一个网络。协调器结点也可以用来在网络中设定安全措施和应用层绑定。协调器的角色主要是启动并设置一个网络，一旦这一工作完成，协调器以一个路由器结点的角色运行。由于 ZigBee 网络具有分布式的特点，网络的后续运行不需要依赖于协调器的存在。

路由器的功能包括允许其他设备加入到网络中，多跳路由和协助用电池供电的终端子设备的通信。路由器需要存储那些去往子设备的信息，直到其子结点醒来并请求数据。当一个子设备要发送一个信息，子设备需要将数据发送给它的父路由结点。此时，路由器就要负责发送数据，执行任何相关的重发，如果有必要还要等待确认。这样，自由结点就可以继续回到睡眠状态。有必要认识到的是，路由器允许成为网络流量的发送方或者接收方。由于这种要求，路由器必须不断准备来转发数据，因此它们通常要用干线供电，而不是使用电池。如有某一工程不需要电池来给设备供电，那么它可以将所有的终端设备作为路由器来使用。一个终端设备并没有维持网络的基础结构的特定责任，所以它可以自己选择是休眠还是激活。终端设备仅在向它们的父结点接收或者发送数据时才会激活。因此，终端设备可以用电池供电来运行很长一段时间。

与移动通信的 CDMA 或 GSM 网络不同的是，ZigBee 网络主要是为工业现场自动化控制数据传输而建立的，因此它必须具有简单、使用方便、工作可靠、价格低的特点。而移动通信网络主要是为语音通信而建立，每个基站造价一般都在百万元人民币以上，而每个 ZigBee 基站却不到 1000 元人民币。每个 ZigBee 网络结点不仅本身可以作为监控对象，例如其所连接的传感器直接进行数据采集和监控，还可以自动中转别的网络结点传过来的数据资料。除此之外，每一个 ZigBee 网络结点（FFD）还可以在自己信号覆盖的范围内和多个没有成为单网络的孤立子结点（RFD）建立无线连接。

4. ZigBee 的自组织网通信方式

ZigBee 技术所采用的自组织网是怎么回事？举一个简单的例子就可以说明这个问题。当一队伞兵空降后，每人持有一个 ZigBee 网络模块终端。降落到地面后，只要他们彼此间在网络模块的通信范围内，通过彼此自动寻找，很快就可以形成一个互联互通的 ZigBee 网络。而且，由于人员的移动，彼此间的联络还会发生变化。与之相似的是模块可以通过重新寻找通信对象，确定彼此间的联络，对原有网络进行刷新，也就是自组织网。

网状网通信实际上就是多通道通信。在实际工业现场，由于各种原因，往往并不能保证每一个无线通道都能够始终畅通，就像城市的街道一样，可能因为车祸、道路维修等原因，使得某条道路的交通出现暂时中断。此时由于我们有多个通道，车辆（相当于我们的控制数据）仍然可以通过其他道路到达目的地，而这一点对工业现场控制而言则非常重要。

所谓动态路由是指网络中数据传输的路径并不是预先设定的，而是在传输数据前，通过对网络当时可利用的所有路径进行搜索，分析它们的位置关系以及远近，然后选择其中的一条路径进行数据传输。在我们的网络管理软件中，路径的选择使用的是“梯度法”，即先选择路径最近的一条通道进行传输，如传不通，再使用另外一条稍远一点的通路进行传输，以此类推，直到数据送达目的地为止。在实际工业现场，预先确定的传输路径随时都可能发生变化，或者因各种原因路径被中断了，或者由于过于繁忙而不能进行及时传送。动态路由结合网状拓扑结构，就可以很好地解决这个问题，从而保证数据的可靠传输。

ZigBee 网络层支持三种网络拓扑结构：星型结构（star）、簇状型结构（ClusterTree）和网状结构（Mesh）。其中簇状结构和网状结构都是属于点对点的拓扑结构，它们是点对点拓扑结构的复杂化形式。

5. ZigBee 的频带

ZigBee 技术主要有以下三种频率与使用范围。

1）868MHz，传输速率为 20Kbps，适用于欧洲；

2）915MHz，传输速率为 40Kbps，适用于北美；

3）2.4GHz，传输速率为 250Kbps，全球通用。

由于此三个频带物理层并不相同，其各自信道带宽也不同，分别为 0.6MHz、2MHz 和 5MHz，分别有 1 个、10 个和 16 个信道。

不同频带的扩频和调制方式有区别，虽然都使用了 DSSS 方式，但从比特到码片的变换方式有较大的差别。调制方式都用了调相技术，但 868MHz 和 915MHz 频段采用的是二相相移键控（Binaary Phase Shift Keying，BPSK），而 2.4GHz 频段采用的是偏移四相相移键控（Offset Quadrature Phase Shift Keying，OQPSK）。在发射功率为 0dBm 的情况下，蓝牙（Bluetooth）通常能达到 10m 的作用范围，而基于 IEEE802.15.4 协议的 ZigBee 在室内通常能达到 30～50m 的作用距离，在室外如果障碍物少，甚至可以达到 100m 的作用距离。

DSSS 是一种扩频通信技术，用高速率的伪噪声码序列与信息码序列模二加（波形相乘）后的复合码序列去控制载波的相位而获得直接序列扩频信号。即将原来较高的功率、较窄的频率变成具有较宽频的低功率频率，以在无线通信领域获得令人满意的抗噪声干扰性能。

BPSK 是把模拟信号转换成数据值的转换方式之一，是利用偏离相位的复数波形组合来表现信息键控移相方式的一种。BPSK 使用了基准的正弦波和相位反转的波形，使一方为 0，另一方为 1，从而可以同时传送和接收 2 值（1bit）的信息。由于最单纯的键控移相方式虽抗噪声较强但传送效率差，所以常常利用 4 个相位的四相相移键控（QPSK）和 8 个相位的 8PSK。移相键控分为绝对移相和相对移相两种，以未调载波的相位作为基准的相位调制叫作绝对移相。以二进制调相为例，取码元为“1”时，调制后载波与未调载波同相；取码元为“0”时，调制后载波与未调载波反相；取码元为“1”和“0”时，调制后载波相位差 180°。

6. ZigBee 性能

1）数据传输速率：比较低，在 2.4GHz 的频段只有 250Kbps，而且只是链路上的速率，除掉信道竞争应答和重传等消耗，真正能被应用所利用的速率可能不足 100Kbps，并且余下的速率可能要被邻近多个结点和同一个结点的多个应用瓜分，因此不适合做视频之类的事情，而适合用于传感和控制领域。

2）可靠性：在可靠性方面，ZigBee 有很多方面进行保证，物理层采用了扩频技术，能够在一定程度上抵抗干扰，介质访问控制（MAC）层（APS 部分）有应答重传功能，MAC 层的载波监听多路访问（CSMA）机制使结点发送前先监听信道，可以起到避开干扰的作用。当 ZigBee 网络受到外界干扰而无法正常工作时，整个网络可以动态地切换到另一个工作信道上。

3）时延：由于 ZigBee 采用随机接入 MAC 层，且不支持时分复用的信道接入方式，因此不能很好地支持一些实时的业务。

4）能耗特性：能耗特性是 ZigBee 的一个技术优势。通常 ZigBee 结点所承载的应用数据速率都比较低，在不需要通信时，结点可以进入很低功耗的休眠状态，此时能耗可能只有正常工作状态下的千分之一。一般情况下，休眠时间占总运行时间的大部分，有时正常工作的时间还不到百分之一，因此可达到很好的节能效果。

5）组网和路由性（即网络层特性）：ZigBee 具备大规模的组网能力，每个网络有 60000 个结点，而蓝牙为每个网络 8 个结点。因为 ZigBee 底层采用了直扩技术，所以如果采用非信标模式，网络可以扩展得很大。因为不需同步，结点加入网络和重新加入网络的过程很快，一般可以做到 1s 以内，甚至更快，而蓝牙则通常需要 3s。在路由方面，ZigBee 支持可靠性很高的网状网的路由，所以可以布置范围很广的网络，并支持广播特性，能够给丰富的应用带来有力的支持。

7. ZigBee 技术优点与应用

Zigbee 技术优点：

1）低功耗：在低耗电待机模式下，2 节 5 号干电池可支持 1 个结点工作 6～24 个月，甚至更长时间，这是 ZigBee 的突出优势。相比较，蓝牙能工作数周，Wi-Fi 可工作数小时。

2）低成本：通过大幅简化协议（不到蓝牙的 1/10），降低了对通信控制器的要求。按预测分析，以 8051 的 8 位微控制器测算，全功能的主结点需要 32KB 代码，子功能结点少至 4KB 代码，而且 ZigBee 免协议专利费，每块芯片的价格大约为 2 美元。

3）低速率：ZigBee 工作在 20～250Kbps 的较低速率，分别提供 250Kbps、40Kbps 和 20Kbps 的原始数据吞吐率，满足低速率传输数据的应用需求。

4）近距离：传输范围一般介于 10～100m 之间，在增加 RF 发射功率后，也可增加到 1～3km。这是指相邻结点间的距离，如果通过路由和结点间通信的接力，传输距离将可以更远。

5）短时延：ZigBee 的响应速度较快，一般从睡眠转入工作状态只需 15ms，结点连接进入网络只需 30ms，进一步节省了电能。相比较，蓝牙需要 3～10s，Wi-Fi 需要 3s。

6）高容量：ZigBee 可采用星型、树型和网状网络结构，由一个主结点管理若干子结点，最多一个主结点可管理 254 个子结点。同时主结点还可由上一层网络结点管理，最多可组成 65000 个结点的大网。

7）高安全：ZigBee 提供了三级安全模式，包括无安全设定、使用接人控制清单（ACL）防止非法获取数据以及采用高级加密标准（AESl28）的对称密码，以灵活确定其安全属性。

8）免执照频段：采用直接序列扩频在工业科学医疗（LSM）频段，2.4GHz（全球）、915MHz（北美）和 868MHz（欧洲）。

8. ZigBee 典型应用

ZigBee 技术应用主要针对工业、家庭自动化、遥测遥控、汽车自动化、农业自动化和医疗护理等，例如灯光自动化控制、传感器的无线数据采集和监控、油田、电力、矿山和物流管理等应用领域。除此这外，它还可以对局部区域内移动目标例如城市中的车辆进行定位。具体应用领域如下：

1）监控照明、HVAC 和写字楼安全；

2）配合传感器和激励器对制造、过程控制、农田耕作、环境及其他区域进行工业监控；

3）带负载管理功能的自动抄表（AMR），这可使得地产管理公司削减成本和节省电气能源；

4）对油气等生产、运输和勘测进行管理；

5）家庭监控照明、安全和其他系统；

6）对病患、设备及设施进行医疗和健康监控；

7）军事应用，包括战场监视和军事机器人的控制；

8）汽车应用，即配合传感器网络报告汽车的所有系统的状态；

9）消费电子应用，包括对玩具、游戏机、电视、立体音响、DVD 播放机和家电设备进行遥控；

10）用于计算机外设，例如键盘、鼠标、游戏控制器及打印机；

11）有源 RFID 应用，如电池供电标签，可用于产品运输、产品跟踪、存储较大物品和财务管理；

12）基于互联网的设备之间的机器到机器（M2M）的通信。

ZigBee 的典型应用如图 4-16 所示。

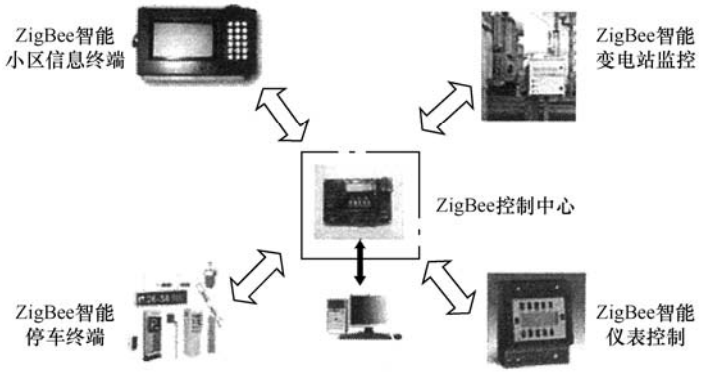


图 4-16　ZigBee 的典型应用

9. ZigBee 实际应用案例

（1）基于 ZigBee 的城市智能公交网络系统

在一个城市的发展规划中，交通的治理是政府工作中的首要大事，而公共交通的发展更是关系到城市交通是否便利的关键。我国目前使用最为广泛的公共交通工具还是公交车，因此发展智能公交是必然趋势。众所周知，普通的公交站牌仅能为乘客提供公交路线信息，而不能提供乘客同样关心的车辆位置信息。随着社会节奏的加快，这种不便因素越来越困扰人们，从而影响人们对出行方式的选择。于是，以 GPS 配合控制中心的智能公交系统应运而生：在公交车上安装 GPS，为控制中心提供车辆位置信息；控制中心再通过有线网络或 GPRS 网络反馈到电子站牌，显示车辆到达的信息。这样的系统虽可以提供车辆位置信息，但是仍存在以下不足：

① 站牌显示的到达时间存在较大误差。由于路况、定位精度、信息刷新时间、信息处理传送时间等因素的影响，所显示时间精确度较差，乘客对这样的信息无法重视。

② 整个系统的成本很高。每辆公交车安装 GPS 和无线数据传输系统，构建一个庞大

的监控中心和带有无线接收系统的点阵显示站牌，几条路线成本就几百万。此外，还需不断投入运行维护的费用，例如在使用 GPRS 通信的站牌系统中，每辆车需要缴纳 GPRS 包月的费用。

③ 系统过于复杂，可靠性有所下降。保证所有公交车辆和站牌都能与中心通信，且不受阻碍是较困难的。一旦任何一方联系中断，站牌信息就无效了。

④ 易受到破坏。这种站牌成本高，可能会成为一些不法分子盗窃的对象，已有媒体报道几万元的站牌遭到破坏的新闻。

系统工作过程简述如下：当车辆 1 到达某站 A 时启动车载发射机，发出车辆到达信号，其内容包含车辆识别信息、乘客状况等。由站牌内处理器记录到达时间，并由 A 站发射机发送该车辆到达 A 站的信息，其信号通过无线网络可到达该车辆运行方向的下一站（A+1 站）。A+1 站接收到车辆到达 A 站的信息后，处理器根据所收到的信息，驱动显示系统显示车辆到达 A 站，同时转发此信息给下一站。下一站（A+2 站）收到信息后，信息处理方式与 A+1 站相同。直到该线路前一趟车（车 2）即将到达的站点 A+n 站收到此信息，它将不再转发该信息（此时它应负责转发车 2 的即将到站信息）。

ZigBee 网络在树型结构下网络的深度不能过大，而采用网型结构又无法进行有效管理，因此不可能只使用一个 ZigBee 网络来实现一个城市的公交系统。这里采用划分多个 ZigBee 网络区域，采用边界路由的方法完成数据的传送，从而形成覆盖城市内所有公交线路的 ZigBee 系统。

每个区域采用树型的网络拓扑结构，以适应公交线路的形状，同时具有固定路由节省存储空间的优点。图 4-17 中，虚线框里是此区域内的一个 ZigBee 传送网络，网络协调器单独安置在中心区域（不作为站牌），其他结点均为站牌。就每条路而言，一侧的站牌为 FFD，作为路由器；另一侧的站牌为 RFD，与路对面的 FFD 站牌通信。在该 ZigBee 网络内，网络成树型拓扑，根为网络调器，同时也为其附近的站牌转发数据。其他站牌按照固定的路由表发送数据，每个 FFD 站牌存有相邻 FFD 的网络地址，数据转发可按此地址逐个进行。该 ZigBee 网络可以覆盖任何通过此区域的公交车路线。为与相邻的 ZigBee 网络通信，在交界处（图 4-17 虚线处）使用装有两个 FFD 模块的边界站牌，作为边界路由器。边界站牌内的两个 ZigBee 模块，分别属于相邻的两个 ZigBee 网络，它们以 SPI 总线的形式与处理器相连，实现多个 ZigBee 网络通信。多个区域相互通信，从而可以覆盖任何一条公交车路线。

图 4-17 只是示意图，具体实施要根据城市道路情况和车辆路线分布作相应的调整，同时可以适当扩大树型结构范围，适当时候可以使用树型、网型混合结构，这需要芯片装载两种路由算法。网络分布规划一般可以遵循以下原则：公交主干线尽量使用较长的 ZigBee 路径，边界站牌应处于两个交通路口中间地段的站牌上。这样可以提高效率，同时边界路

由程序设计上相对容易。

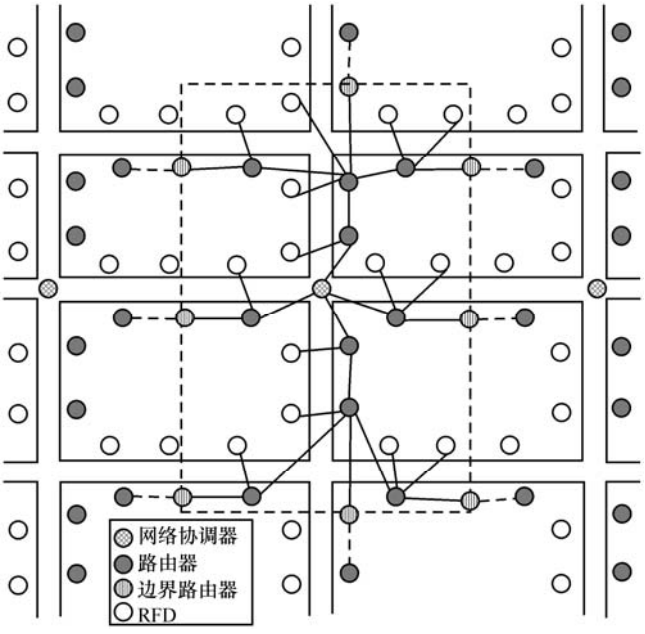


图 4-17　站牌信息传送网络拓扑图

ZigBee 结点在移动中网络和路由的变化都需要网络协调器管理，因此将产生多次与网络协调器的通信。为了减少 ZigBee 信道相互之间的干扰，同时简化处理单元的任务，车载 ZigBee 模块和站牌车辆信息 ZigBee 模块将使用不同于站牌之间信息交换的 ZigBee 通信信道。它们形成的网络与图 4-17 所示的站牌信息传送网络相独立。该网络中，每个站牌车辆信息 ZigBee 模块作为网络协调器，与停靠此站车辆的车载 ZigBee 模块组成星型的 ZigBee 网络，网络范围为 70m 左右。

（2）ZigBee 智能交通系统方案（ZigBee 应用）

近年来，利用先进的科学技术改造城市交通系统已成为城市交通管理者的共识。交通信号的调整是随时随地都需要的。现有的红绿灯控制系统在铺设时其控制线路须专门挖道布线，给整个交通调度带来很大的不便。同时，这种挖道布线方式费用相应较高，日后的维护保养也十分不便。当出现交通堵塞等紧急状况时，需要交警在现场及时而灵活调整红绿灯的时间设置，而现有系统只能预先设置几个固定模式，无法达到根据具体情况设置的要求。此外，主管部门也希望能及时了解每个路口的交通状况和红绿灯状况，这就需要设备之间实现网络的互联互通，而传统的有线方式面临着布线困难、维护不易、成本较高等问题。ZigBee 智能交通系统示意图，如图 4-18 所示。

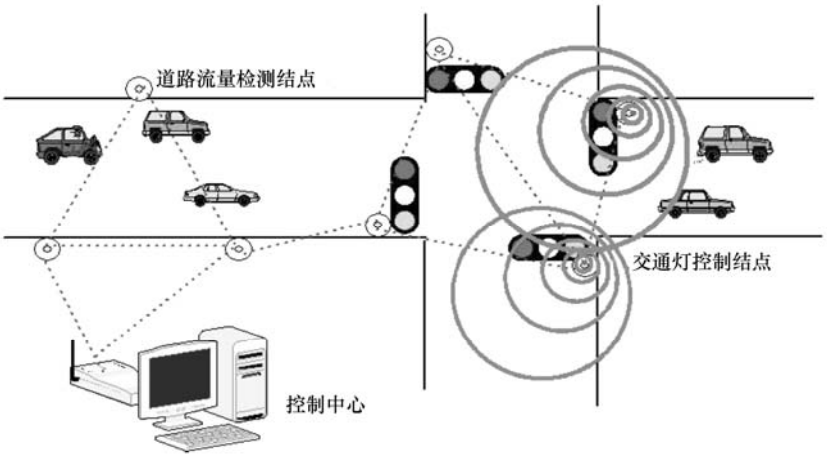


图 4-18　ZigBee 智能交通系统示意图

系统特点：

- 无须挖路布设控制线路，各设备之间实现无线自动组网连接，降低了系统安装成本，避免了传统安装方式因交通干扰所带来的经济损失。
- 由于系统没有地面控制箱和控制线路，避免了恶意破坏；而且整个控制系统的各个模块具有高集成度，高可靠性和低功耗、低成本、体积小等优点，维护保养十分方便，只需更换相应结点即可，避免了传统控制线路本身带来的许多麻烦，从而大大减少了设备购置成本、建设安装成本和系统维护成本。
- 卓越的物理性能。每个模块的无线连接距离，根据需要可从几十至几百米，甚至几公里。整个网络所使用的无线频率是国际通用的免费频段（2.4～2.48GHz ISM）。

（3）基于 ZigBee 的无线传感器网络在大型停车场中的应用

在商场、超市、车站、机场、地铁出口、医院、大型小区，都配套有拥有约 300 个甚至上千个停车位的大型停车场。人工收费和管理已经无法满足快速、高效、安全管理的需求，组建基于 ZigBee 的无线传感器网络，将帮助物业管理部门对大型停车场进行有效的管理。

该系统可分为四个模块：入口管理、泊位管理、出口与收费管理、管理中心。

中央监控计算机对来自停车场的所有数据集中处理，并返回相对应的操作指令。在协调和管理整个监控系统的同时，也可通过系统集成，融入小区、大楼的智能自动化管理系统。在需要时，可向上级管理部门提供数据包表或具体的车辆定位查询。

停车场本身可标记为 A、B、C 等多个区，每个区可设置一个 ZigBee 路由。每个车位可设置一个基于ec2430模块的精简功能无线传感器终端，每个路由管理该区的数十个终端，

整个 Mesh 网络由一个协调器来协调，并与中央监控系统交换信息，停车场的各个结点的拓扑结构如图 4-19 所示。

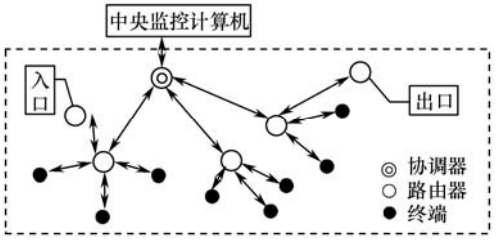


图 4-19　停车场各结点拓扑结构图

停车场的客户可分月租和临时两种：月租客户随车携带停车卡；临时客户在发卡处领取停车卡，出口处交还。停车卡中选用 TI 公司生产的基于 ZigBee 技术的带定位引擎的射频芯片 CC2431。

1）入口管理。

入口部分主要由 ZigBee 路由器、发卡机（或管理员）、车位显示屏、摄像头、电动栏杆、挡车器组成。其控制原理如图 4-20 所示。

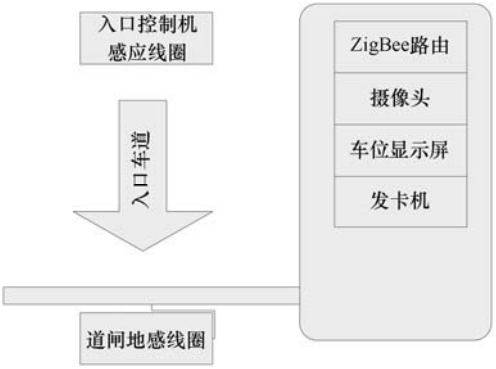


图 4-20　入口控制原理图

月租客户的车行驶至离入口 10m 处时，ZigBee 路由就能接收到停车卡的射频信号。路由得到射频卡芯片的 64 位全球唯一的 MAC 地址后，由协调器为该终端分配一个 16 位网络地址。停车卡终端以此地址与 ZigBee 网络中其他设备进行通信。中央控制计算机得到停车卡的 MAC 地址后，核对该停车卡的使用情况。如该卡已被某车位匹配使用，则管理员或发卡机提示车主另取临时付费卡使用。车辆进入 El 车道缓慢行驶时，可观察车位显示屏中空闲车位的分布情况。同时，摄像头将车牌拍下并传输给中央控制计算机。计算机运行

识别系统软件，识别出车牌，同时将此车所使用或将使用的停车卡的 MAC 地址及停车时间存入系统。月租客户核对无误后，电动栏杆自动起栏放行车辆；如为临时客户，将在取卡后放行，待车辆通过后，再放下栏杆。

2）泊位管理。

车辆进入停车场后，可自主选择车位泊车。泊位管理由泊位分布显示屏、泊位指示器、各种智能路标、车位无线传感器、ZigBee 路由器等组成。

车辆进入某块区域时，基于接收信号强度（RSSI）的定位技术，车辆里的停车卡中的 cc2431 芯片可以与周边的车位传感器中的 cc2430 芯片一起定位并回报中央控制计算机其位置。目前采用不同的算法，精度可控制在 0.5～3m 的误差范围内。但停车场车位与车位间距离较近，如精确匹配停车卡和车位，需要提供更多信息。目前超声波定位技术、射频识别技术成本都相对较高。本系统中，采用廉价的红外线反射性传感器与 cc2430 相结合的方法。

车辆停车后，红外线反射性传感器感应到车辆，cc2430 芯片将车位已泊车的信息通过 ZigBee 网络传给中央控制计算机。中央计算机系统比对停车卡 cc2431 芯片定位的数据后，将车位编号、停车卡编号、车牌、停车起始时间等作为一条记录保存下来，同时发出指令，修改入口处等地的车位显示屏。车辆离开车位时，cc2430 芯片将车位空闲的信息报告中央控制计算机；同时，核对原停车卡是否连入该区域，如果没有，立刻启动防盗警戒系统，阻止车辆离开。

各车位的无线传感器因为处理的信息较简单，可采用精简的功能终端设备。红外线传感器可连接倒车警告电路。同时，设定各区域的某一个终端增加温度或有害气体传感器，以预防火灾或监控其他的安全问题。

3）出口管理和收费。

出口管理主要由 ZigBee 路由器、收费管理窗口、信息显示屏、摄像头、电动栏杆、挡车器组成。其控制原理如图 4-21 所示。

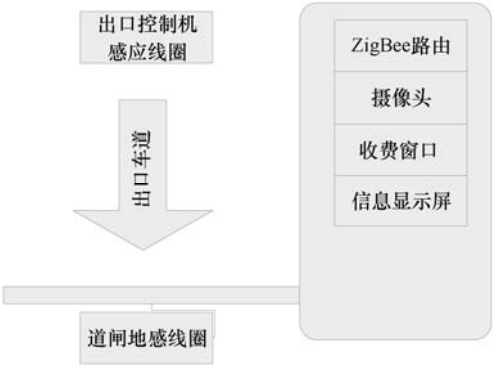


图 4-21　出口收费控制原理图

月租车辆在出口车道时，ZigBee 路由检测到新的终端即停车卡，摄像头拍得车牌信息，在系统识别并与原记录中保存的车牌对比无误后，通知道闸，启动电动栏杆，车辆离开停车场。

临时车辆进入出口车道时，ZigBee 路由检测到停车卡，将该车辆停车终止时间返回中央控制系统。中央控制系统根据停车时间、费率等计算出停车费，将信息通过网络传给收费管理窗口和信息显示屏，收费员在回收停车卡并完成收费后，启动电动栏杆，放行车辆。

4）管理中心系统。

管理中心的功能是管理和监控停车场的出口、入口、停车位的运行使用和安全情况。系统包括：管理月租卡和临时卡的使用；管理月租卡客户的有关信息；设置收费费率，并生成各种财务报表；实时管理车位信息，更新各处显示屏，临时停车位已满时，在显示屏上显示无空车位，暂停临时客户车辆的泊车；月租客户期限将满时提醒续费；对停车情况进行汇总分析，最大可能地提高停车场的利用率；通过分布各处的传感器，保证消防安全；管理排风机等设备，及时换气；通过摄像头等方式，最大可能地保障停车场的安全防盗工作，在必要时，可向警方随时提供精确到车位的车牌查询。

（4）基于 ZigBee 技术的无线消防报警定位系统

网络拓扑结构如图 4-22 所示。ZigBee 协调器、中继器（路由器）和终端设备以边缘为星型的网状拓扑方式连接。当网络中某处物理位置发生火警时，其附近传感器结点感测到火警并将其通过网络传播出去。进入火灾现场的消防人员随身携带嵌入了无线模块的移动装置，这种移动装置被视为网络中的移动结点，它通过向其周围固定安装的位置已知的结点发送测量命令消息，接收到消息的结点通过其中所包含的信息可估算位置未知的移动结点所在位置。网络协调器可将网络信息传送到 PC 中，从而可了解网络结点工作情况以及消防人员的位置。

要组建一个基于 ZigBee 技术的无线消防报警定位系统，首先要对数据进行采集和处理，例如环境感测数据；然后要实现结点间的通信，才能将获得的信息从一个结点传送到其他结点；最后要进行组网以及定位估计，才能最终实现一个自组织网络并对移动未知结点进行定位。

要组建一个基于 ZigBee 技术的无线消防报警定位系统，首先要对数据进行采集和处理，例如环境感测数据；然后要实现结点间的通信，才能将获得的信息从一个结点传送到其他结点；最后要进行组网以及定位估计，才能最终实现一个自组织网络并对移动未知结点进行定位。

根据以上分析，可将系统软件大致分为以下几个部分。

1）数据采集与传输：包括温度数据采集、通信方式、数据格式与传输机制。

2）组网及路由：网络的建立、结点加入以及路由算法的设计与实现。

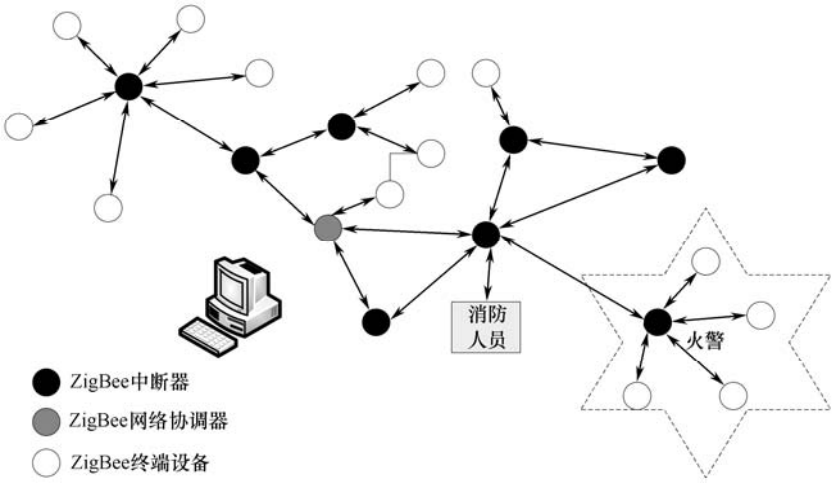


图 4-22　ZigBee 无线消防报警网络拓扑示意图

3）定位算法：算法原理、门限设置。

系统中的基本单元有感测单元、处理单元、能量单元和数据收发单元，此外还包含了移动设备和定位系统。具体到本设计中，感测、处理、能量和数据收发四个单元在结点硬件上都有相对独立的模块。而移动和定位功能则融合在这些模块当中，无独立硬件模块。结点分为固定安装结点和可移动结点，位置固定的结点构成本系统的网络主体，建立一个独立运行的网状网络，在系统中被称为参考结点；移动的结点嵌入在消防人员随身携带的移动装置中，在系统中被称为目标结点。位则由处理单元和数据收发单元配合实现。

4.5.2　Wi-Fi

1. Wi-Fi 概念

所谓“Wi-Fi”其实就是 Wireless Fidelity 的缩写，意思就是无限局域网。由于 Wi-Fi 产品的标准是遵循 IEEE 所制定的 802.11x 系列标准，所以一般所谓的 802.11x 系列标准都属于 Wi-Fi。而目前最流行的标准就是 802.11b，也就是无线的标准协议。该标准从 802.11 的 2MB 基础带宽增加到 11MB，达到局域网水平，而且 802.11g 还可以兼容 802.11b，因此成为市场新贵。

Wi-Fi 技术从提出到现在已经在电信业和 IT 业引起了广泛的关注和应用。英特尔花费了近 20 亿美元开发、推广自带无线网络模块的迅弛笔记本处理器，由此可见 Wi-Fi 将在近几年内得到极大的发展，而且还预示着这是一个不可逆转的方向。

目前，许多的固定、移动电话运营商都已杀入这块市场。国际上已经有许多的移动运营商们争先恐后地向用户提供付费 Wi-Fi 服务。斯普林特（Sprint）已向从事 Wi-Fi 技术的

公司 BoingoWireless 进行投资，并宣布将与 Wyndham International 酒店合作，部署 Wi-Fi 热点。凌志达通讯有限公司（Nextel Communications Inc）正与摩托罗拉公司（Motorola Inc）合作开发 Wi-Fi 手机，并向一家为企业部署用于 Wi-Fi 和手机移动通信网络的公司 Radio Frame Networks Inc 提供支持。

2003 年 3 月 17 日，美国最大的移动运营商 Verizon 无线宣布将在机场、酒店等室内热点地区提供 Wi-Fi 无线接入服务。同时 AT&T 无线、T-Mobile 美国公司也在积极进行 Wi-Fi 接入铺设。Nextel 公司则选择面向大企业客户，主要在该公司手机用户基础上开展 Wi-Fi 业务。各大公司的介入，表明了 Wi-Fi 技术的无限前景。

而事实证明 Wi-Fi 技术在全球的商用范围很广，用户数量巨大，有较广泛的应用，除了运营商经营以外，包括政府、企业和个人在内，在公共场合、企业内部、家庭都有应用。到 2006 年年底，全球 Wi-Fi 的芯片出货总量达到了 5 亿块，在全球 100 多个国家有超过 6 万个热点。因此，Wi-Fi 的用户基础良好，仅次于 3G 技术。

由此可见，Wi-Fi 作为传统以太网的无线延伸有可能实现人们一直追求的“无处不在的移动宽带时代”，随着厂家的大力推广、技术的不断改进，必将成为无线通信的另一种选择，也必然掀起无线通信领域的大变革。但要真正实现电信级 Wi-Fi 网络的部署和应用，对于国内的运营商而言，既存在着挑战又存在着机遇。国内运营商也应该把握该技术所带来的机会，从而在无线通信领域拓展出更广阔的利润空间。

2. Wi-Fi 技术的发展与特点

（1）Wi-Fi 技术的发展

Wi-Fi 产品的标准是遵循 IEEE——美国电工电子技术协会所制定的 802.11 系列标准，它是美国电机电子工程师协会为解决无线网络设备互连，于 1997 年 6 月制定发布的无线局域网标准。所以一般所谓的 802.11X 系列标准都属于 Wi-Fi。

IEEE 802.11 主要用于解决办公室局域网和校园中用户与用户终端的无线连接，其业务主要局限于数据访问，速率最高只能达到 2Mbps。由于它在速率和传输距离上都不能满足人们的需要，因此 IEEE 又相继推出了 802.11b、802.11a 和 802.11g3 个新标准，下面分别进行简要的介绍。

IEEE 802.11 标准的制定推动了无线网络的发展，但由于传输速率只有 1~2Mbps，该标准未能得到广泛的发展与应用。1999 年，IEEE 通过了新的 IEEE 802.11a 和 IEEE 802.11b 标准。IEEE 802.11b 定义了使用直接序列扩频调制技术，在 2.4GHz 频带实现速率为 11Mbps 的无线传输。由于 DSSS 技术的实现比 OFDM 容易，IEEE 802.11b 标准的发展比 IEEE 802.11a 快得多，在 1999 年年末首先出现了支持 IEEE 802.11b 标准的产品，随后得到广泛商用，并通过互通性测试。IEEE 802.11b 已成为当今 WLAN 的主流标准。

随着用户需求的增加，又诞生了 IEEE 802.11a 标准，该标准工作在 5GHz 频段，最大速

率可达 54Mbps。采用 OFDM 调制技术的 IEEE 802.11a 标准与 IEEE 802.11b 相比，具有两个明显的优点：第一，提高了每个信道的最大传输速率（11~54Mbps）；第二，增加了非重叠的信道数。因此，采用 IEEE 802.11a 标准的 WLAN 可以同时支持多个相互不干扰的高速 WLAN 用户。不过这些优点是以兼容性和传输距离为代价。IEEE 802.11a 和 IEEE 802.11b 工作在不同的频段，两个标准的产品不能兼容。由于传输距离的减小，要覆盖相同的范围，就需要更多的 IEEE 802.11a 接入点。2002 年年初，首次出现了支持 IEEE 802.11a 标准的产品。

2001 年 1 月，IEEE 802.11g 标准以草案的形式面世，在 2003 年 5 月已成为正式标准。IEEE 802.11g 标准既能提供与 IEEE 802.11a 相同的传输速率，又能与已有的 IEEE 802.11b 设备后向兼容。IEEE 802.11g 也工作在 ISM2.4GHz 频段，在速率不大于 11Mbps 时，仍采用 DSSS 调制技术；当传输速率高于 11Mbps 时，则采用传输效率更高的 OFDM 调制技术。与 IEEE 802.11a 相比，IEEE 802.11g 的优点是以性能的降低为代价的。虽然 OFDM 调制技术能达到更高的速率，但 2.4GHz 频带的可用带宽是固定的，IEEE 802.11g 只能使用 2.4Hz 频段的 3 个信道，而 IEEE 802.11a 在 5GHz 频带室内/室外可用的信道各有 8 个。由于 IEEE 802.11a 的可用信道数比 IEEE 802.11g 多，在相同传输速率下，频道重叠少，干扰就小。所以，IEEE 802.11a 与 IEEE 802.11g 相比，具有较强的抗干扰能力。

（2）现有 Wi-Fi 技术特点

Wi-Fi 标准在设定时就有自身所带的一些优点和缺点。其主要问题是：第一，在 Wi-Fi 标准中，802.11b 是目前最广泛使用的标准，目前的产品中，支持此标准的产品比支持 802.11a 和 802.11g 的产品便宜，但也是 Wi-Fi 标准中带宽最低、传输距离最短的一个标准。第二，802.11a 比 802.11b 具有更大的吞吐量，可同时使用多个频道以加速传输速率，电波不易受干扰，传输速率也很快达 54Mbps，但由于它的工作频率在 5GHz，与 802.11b 和 802.11g 不兼容（此二者工作于 2.4GHz），所以它是目前使用较少的一个 Wi-Fi 标准。第三，802.11g 的传输速率（理论上达 54Mbps）比 802.11b（理论上为 11Mbps）要高，并且可与之兼容，但是它却比 802.11b 更容易受外界干扰，如无绳电话、微波炉及其他在 2.4GHz 频段上的设备。

最后就是在安全性上的问题，一般的无线设备在传播信息时所使用的无线信号可被其他人侦听到，并且目前常用的 802.11b 和 802.11g 工作在免费的通用频段之内，所以 Wi-Fi 无线设备在设计的过程中必须要考虑到安全保密的内容。目前所生产的无线设备中大多数采用的是 40/128 位的 WEP，部分产品支持 VPN 技术，在安全性方面已达到了一定的水平，但随着技术的发展，安全性方面还有待改进。

3. Wi-Fi 技术的原理

Wi-Fi 技术是目前最主流的无线网络标准，虽然标准在很久以前就已经制定了，但是由于因技术不成熟所导致的传输速度慢（遗失数据严重），使得市场接收程度偏低。不过自从英特尔公司向市场推出名为迅驰（Centrino）的无线整合技术后，整个无线网络市场

又被重新挖掘出来。Wi-Fi 正逐渐走向成熟，下面就来介绍下这种逐渐被社会认可的技术的系统原理。

（1）Wi-Fi 技术性能指标和关键技术

现在无线网通信协议主要采用的标准是 IEEE 802.11b、IEEE 802.11a 和 IEEE 802.11g。表 4-1 是它们三者间的比较。

表 4-1　性能指标比较

标　　准	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a
工作频段/GHz	2.4	2.4，5	5
数据速率/Mbps	1，2，5.5，11	1，2，5.5，11，6，12，24；9，18，36，48，54	6，12，24，9，18，36，48，54
覆盖范围/m	150～300	50～150	30

在无线局域网市场中，802.11a 产品在国外使用广泛，在国内 802.11b 是无线局域网的主流标准，802.11g 因速率高及与 802.11a 和 802.1lb 兼容受到了青睐。从发展来看，今后应采用双频三模（802.11a/b/g）的产品。双频三模无线产品不但可工作在与 802.1la 相同的 5GHz 频段，还可与工作在 2.4GHz 的 802.11b 和 802.1g 产品全面兼容，支持整个 802.11a，b，g 标准、完整互通性单一平台，实现无线标准的互联与兼容。

正如传闻所言，Wi-Fi 所遵循的 802.11 标准是以前军方所使用的无线电通信技术，而且至今还是美军军方通信器材对抗电子干扰的重要通信技术。因为，Wi-Fi 中所采用的 SS（SpreadSpectrum，展频）技术具有非常优良的抗干扰能力，并且在需要反跟踪、反窃听时又具有很出色的效果，所以不需要担心 Wi-Fi 技术是否能提供稳定的网络服务。而常用的展频技术有如下四种：DD-SS 直序展频，FH-SS 调频展频，TH-SS 跳时展频，C-SS 连续波调频。在上面常用的技术中，前两种展频技术很常见，也就是 DS-SS 和 FH-SS。后两种则是根据前面的技术加以变化，也就是 TH-SS 和 C-SS 通常不会单独使用，而是整合到其他的展频技术上，组成信号更隐密、功率更低、传输更为精确的混合展频技术。综合来看展频技术有以下方面的优势：反窃听，抗干扰，有限度的保密。DS-SS 的展频过程如图 4-23 所示。

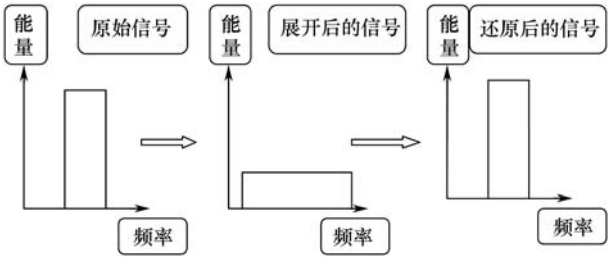


图 4-23　DS-SS 的展频过程

1）直序扩频技术。

直序扩频技术，是指把原来功率较高，而且带宽较窄的原始功率频谱分散在很宽广的带宽上，使得在整个发射信号利用很少的能量即可被传送出去。

在传输过程中把单个 0 或 1 的二进制数据使用多个 chips（片段）进行传输，然后在接收方进行统计 chips 的数量来增加抵抗噪声干扰。例如要传送一个 1 的二进制数据到远程，那么 DS-SS 会把这个 1 扩展成三个 1，也就是 111 进行传送。那么即使是在传送中因为干扰，使得原来的三个 1 成为 011、101、110、111 信号，但还是能通过统计 1 出现的次数来确认该数据为 1。通过这种发送多个相同的 chips 的方式，就比较容易减少噪声对数据的干扰，提高接收方得到数据的正确性。另外，由于所发送的展频信号会大幅降低传送时的能量，所以在军事用途上会利用该技术把信号隐藏在 BackGroundNoise（背景噪声）中，减少敌人监听到的我方通信信号以及频道。这就是展频技术所隐藏信号的反监听功能了。

2）跳频技术。

跳频技术（Frequency-Hopping Spread Spectrum，FH-SS）技术，是指把整个带宽分割成不少于 75 个频道，每个不同的频道都可以单独地传送数据。当传送数据时，根据收发双方预定的协议，在一个频道传送一定时间后，就同步“跳”到另一个频道上继续通信。

FH-SS 系统通常在若干不同频段之间跳转来避免相同频段内其他传输信号的干扰。在每次跳频时，FH-SS 信号表现为一个窄带信号。

若在传输过程中，不断地把频道跳转到协议好的频道上，在军事用途上就可以用来作为电子反跟踪的主要技术。即使敌方能从某个频道上监听到信号，但因为我方会不断跳转其他频道上通信，所以敌方就很难追踪到我方下一个要跳转的频道，达到反跟踪的目的。

如果把前面介绍的 DS-SS 以及 FS-SS 整合起来一起使用的话，将会成为 hybrid FH/DS-SS。这样，整个展频技术就能把原来信号展频为能量很低、不断跳频的信号。使得信号抗干扰能力更强、敌方更难发现，即使敌方在某个频道上监听到信号，但信号不断地跳转频道使敌方不能获得完整的信号内容，完成利用展频技术隐密通信的任务。

FH-SS 系统所面临的一个主要挑战便是数据传输速率。就目前情形而言，FH-SS 系统使用 1MHz 窄带载波进行传输，数据速率可以达到 2Mbps，不过对于 FH-SS 系统来说，要超越 10Mbps 的传输速率并不容易，从而限制了它在网络中的使用。

3）OFDM 技术。

它是一种无线环境下的高速多载波传输技术。其主要思想是：在频域内将给定信道分成许多正交子信道，在每个子信道上使用一个子载波进行调制，各子载波并行传输，从而能有效地抑制无线信道的时间弥散所带来的符号间干扰（ISI），这样就减少了手机内均衡的复杂度，有时甚至可以不采用均衡器，仅通过插入循环前缀的方式消除 ISI 的不利影响。

OFDM 技术有非常广阔的发展前景，已成为第四代移动通信的核心技术。IEEE 802.11a，

g 标准为了支持高速数据传出都采用了 OFDM 调制技术。目前，OFDM 结合时空编码、分集、干扰（包括符号间干扰 ISI）和邻道干扰（ICI）抑制以及智能天线技术，最大限度地提高了物理层的可靠性。如再结合自适应调制、自适应编码以及动态子载波分配和动态比特分配算法等技术，可以使其性能进一步优化。

（2）Wi-Fi 的协议及 MAC 层关键技术

1）CSMA/CA 协议。

总线型局域网在 MAC 层的标准协议是 CSMA/CD，但是由于无线产品的适配器不易检测信道是否存在冲突，802.11 定义了一种新的协议，就是 CSM/MA。它一方面经行载波真挺，以查看介质是否空闲；另一方面通过随机的时间等待，使信号冲突发生的概率减到最小，以避免冲突。当侦听到介质空闲时，优先发送。

不仅如此，为了系统更加稳固，802.11 还提供了带确认（ACK）的 CSMA/CA。一旦遭受其他噪声干扰或者在侦听失败时，就有可能发生信号冲突，这种工作于 MAC 层的 ACK 此时能够提供快速的恢复能力。

从理论上来讲，MAC 层的 CSMA/CA 协议完全能够满足局域网级的多用户信道竞争问题。但是，对于无线环境而言，它不像有线广播媒体那样好控制，来自其他 LAN 中的用户传输会干扰 CSMA/CA 的操作。而且，在无线环境中，因为发射设备的功率通常要比接收设备的功率强得多，检测冲突是困难的，因此，不可能终止互相冲突的传输。在这种环境下，设计一个能够帮助避免冲突的系统更为有意义。无线局域网存在隐藏站点的问题，大多数无线电都是半双工的，它们不能在同一频率上发送并同时监听突发噪声，因此，IEEE 802.11 采用了 CSMA/CA 技术，CA 表示冲突避免，这种协议实际上是在发送数据帧前对信道进行预约。

2）BTMA 协议。

BTMA（忙音多路访问）协议就是为解决暴露终端的问题而设计的。BTMA 把可用的频带划分成数据（报文）通道和忙音通道。当一个设备在接收信息时，它把特别的数据即一个“音”放到忙音通道上，其他要给该接收站发送数据的设备在它的忙音通道上听到忙音，知道不要发送数据。使用 BTMA，在上面的例子中，在 B 向 A 发送的同时，C 就可以向 D 发送（假定 C 已感知 B 和 D 不在同一个无线范围内），因为 C 没有在 D 的忙音通道上接收到因其他站的发送而引起的忙音。另外，使用 BTMA，如果 C 在向 B 发送，因为 A 可以在 B 的忙音通道上接收到由于 C 的发送而引起的忙音。所以 A 可以知道而不向 B 发送。在暴露终端的情况下，一个无线覆盖区域中的一个设备检测不到在邻接覆盖区域中的忙音通道上的忙音。

3）MAC 层 IEEE 802.11e 协议。

在 802.11e 中，每一个无线结点成为 QSTA，它可以通过 EDCA 和 HCCA 两种方式访

问信道。其中 EDCA 机制和 802.11DCF 相似，只是针对不同优先级的访问类别有不同的帧间隔和竞争窗口。而在 HCCA 机制中，一个控制结点可以优先访问信道，并调度其他 QSTA 可以获得一段 TXOP 发送多个数据包。

相比于 802.11DCF/PCF，802.11EDCA/HCCA 主要做了以下几个方面的扩充：第一，属于不同优先级的站点在经行二进制回退争抢信道时，需要等待不同的任意帧间隔。与 802.11 DCF 等待相同的 DIFS 时间不同，在 EDCA 中，属于优先级的站点需要等待 AIFS。第二，属于不同优先级的站点在经行二进制回退争抢信道时，所用的最大竞争窗口和最小竞争窗口范围不同。优先级越高，最大竞争窗口的数值越小。因此高优先级的站点其计数器的取值较小，可以更早的递减到 0。第三，引入了虚拟竞争，在同一个站点内部，802.11e 把所有数据包分成 8 类，映射到 4 个接入等级，每一个接入等级都对应站点内部的一个队列，当高优先级的队列和低优先级的队列计数器同时到 0 时，站点内部的调度器会判断出高优先级队列并成功发送，而低优先级队列则进行二进制回退，再次争抢信道。第四，引入了 TXOP，在 820.11e 的 HCCA 机制中，一个控制结点可以优先访问信道，并调度其他 QSTA 对信道访问。

（3）Wi-Fi 技术的结构

1）Wi-Fi 技术的网络结构。

i．参考模型。

无线局域网由端站（STA）、接入点（AP）、接入控制器（AC）、AAA 服务器以及网元管理单元组成，其网络参考模型如图 4-24 所示。AAA 服务器是提供 AAA 服务的实体，在参考模型中，AAA 服务器支持 RADIUS 协议。Portal 服务器适用于门户网站推送的实体，在 Web 认证是辅助功能完成认证功能。

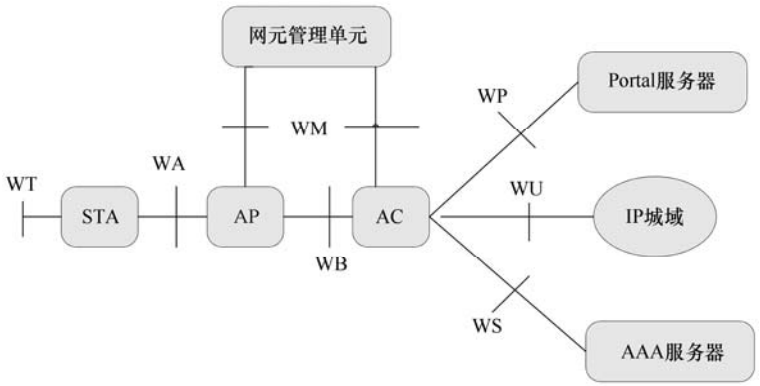


图 4-24　无线局域网网络参考模型

ii．接口定义。

在该网络模型中，定义了如下接口。

① WA 接口：STA 和接入点之间的接口，即空中接口。

② WB 接口：接入点和接入控制器之间的接口，该接口为逻辑接口，可以不对应具体的物理接口。

③ WT 接口：STA 和用户终端的接口，该接口为逻辑接口，可以不对应具体的物理接口。

④ WU 接口：公共无线局域网（PWLAN）与 Internet 之间的接口。

⑤ WS 接口：AC 与 AAA 服务器之间的接口，该接口为逻辑接口，可以不对应具体的物理接口。

⑥ WP 接口：AC 与 Portal 服务器之间的接口，该接口为逻辑接口，可以不对应具体的物理接口。

⑦ WM 接口：公众无线局域网网元管理单元之间的接口，该接口为逻辑接口。

iii．网络单元功能。

在该无线局域网网络参考模型中，各个网络单元的功能如下所述。

① 端站（STA）是无线网络中的终端（可以通过不同接口接入计算机终端），也可以是非计算机终端上的嵌入式设备；STA 通过无线链路接入 AP，STA 和 AP 之间的接口为空中接口。

② 接入点（AP）通过无线链路和 STA 进行通信，无线链路采用标准的空中接口协议，AP 和 STA 均为可以寻址的实体，AP 上行方向通过 WB 接口采用有线方式与 AC 连接。

③ 接入控制器（AC）在无线局域网和外部网之间充当网管功能；AC 将来自不同 AP 的数据进行汇聚，与 Internet 相连；AC 支持用户安全控制、业务控制、计费信息采集及对网络的监控；AC 可以直接和 AAA 服务器相连，也可以通过 IP 城域网骨干网（支持 Radius 协议）相连；在特定的网络环境下，接入控制器 AC 和接入点 AP 对应的功能可以在物理上实现一体化。

④ AAA 服务器具备认证、授权和计费（AAA）功能；AAA 服务器在物理上可以由具备不同功能的独立的服务器构成，即认证服务器（AS）、授权服务器和计费服务器；认证服务器保存用户的认证信息和相关属性，当接收到认证申请时，支持在数据库中对用户数据的查询；在认证完成后，授权服务器根据用户信息授权用户具有不同的属性；在本标准中，AAA 服务器即支持 RADIUS 协议的服务器。

⑤ Portal 服务器负责完成 PWLAN 用户门户网站的推送，Portal 服务器为必选网络单元。

2）Wi-Fi 技术的拓扑结构。

无线局域网的拓扑结构可归纳为两类，即无中心网络和有中心网络。

i．无中心网络。

无中心网络是最简单的无线局域网结构，又称为无 AP 网络，对等网络或 Ad-Hoc（特别）网络，它由一组有无线接口的计算机（无线客户端）组成一个独立基本服务集（IBSS），这些无线客户端有相同的工作组名、ESSID 和密码，网络中任意两个站点之间均可直接通信。无中心网络的拓扑结构如图 4-25 所示。

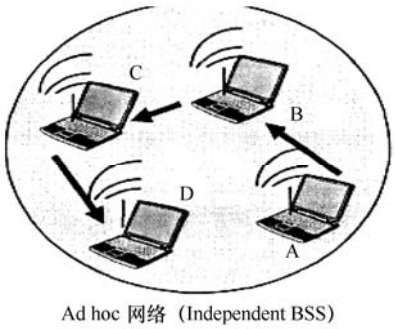


图 4-25　无中心网络的拓扑结构

无中心网络一般使用公用广播信道，每个站点都可竞争公用信道，而信道接入控制（MAC）协议大多采用 CSMA（载波监测多址接入）类型的多址接入协议。这种结构的优点是：网络抗毁性好、建网容易、成本较低。这种结构的缺点是：当网络中用户数量（站点数量）过多时，激烈的信道竞争将直接降低网络性能。此外，为了满足任意两个站点均可直接通信，网络中的站点布局受环境限制较大。因此，这种网络结构仅适应于工作站数量相对较少（一般不超过 15 台）的工作群，并且这些工作站应离得足够近。

ii．有中心网络。

有中心网络也称结构化网络，它由一个或多个无线 AP 以及一系列无线客户端构成，网络拓扑结构如图 4-26 所示。在有中心网络中，一个无线 AP 以及与其关联（Associate）的无线客户端被称为一个 BSS（Basic Service Set，基本服务集），两个或多个 BSS 可构成一个 ESS（Extended Service Set，扩展服务集）。

有中心网络使用无线 AP 作为中心站，所有无线客户端对网络的访问均由无线 AP 控制。这样，当网络业务量增大时，网络吞吐性能及网络时延性能的恶化并不强烈。由于每个站点只要在中心站覆盖范围内就可与其他站点通信，故网络布局受环境限制比较小。此外，中心站为接入有线主干网提供了一个逻辑访问点。有中心网络拓扑结构的弱点是：抗毁性差，中心站点的故障容易导致整个网络瘫痪，并且中心站点的引入增加了网络成本。

虽然在 IEEE 802.11 标准中并没有明确定义构成 ESS 的分布式系统的结构，但目前大都是指以太网。ESS 的网络结构只包含物理层和数据链路层，不包含网络层及其以上各层。因此，对于 IP 等高层协议 IP 来说，一个 ESS 就是 IP 子网。

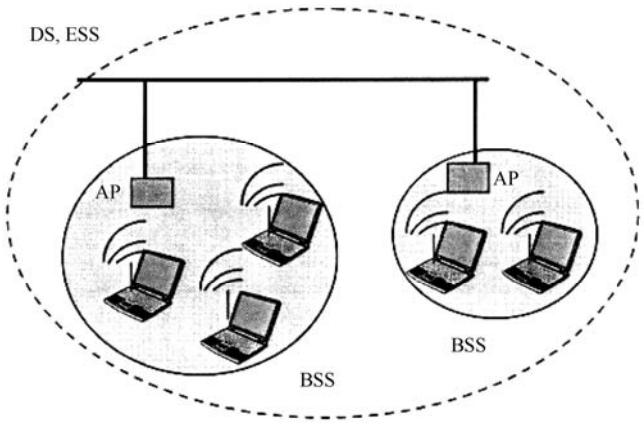


图 4-26　有中心网络的拓扑结构

（4）Wi-Fi 的传输方式

传输方式设涉及无线局域网采用的传输媒体、选择的频段及调制方式。目前，无线局域网采用的传输媒体主要有两种，即微波与红外线。按照不同的调制方式，采用微波作为传输媒体的无线局域网又可分为扩展频谱方式与窄带调制方式。微波和红外线都属于电磁波。

1）局域网。

i．红外线（Intrared Rays，IR）局域网。

近年来，基于红外线的传输技术有了很大发展，目前广泛使用的家电遥控器几乎都采用红外线传输技术。红外线传输技术采用波长小于 1μm 的红外线作为传输媒体，有较强的方向性。由于它采用了低于可见光的部分频谱作为传输媒体，因此使用不受无线电管理部门的限制。红外信号要求视距（直观可见距离）传输，因此很难被窃听，对邻近区域的类似系统也不会产生干扰。

作为无线局域网的传输方式，采用红外线通信方式与微波方式比较，可以提供极高的数据传输速率，有较高的安全性，且设备相对简单、便宜。但由于红外线对障碍物的透射和绕射能力很差，使得传输距离和覆盖范围都受到很大限制，通常 IR 局域网的覆盖范围被限制在一间房屋内。另外，在实际应用中，由于红外线具有很高的背景噪声，受日光、环境照明等影响较大，一般信号源设备的发射功率要大一些。

ii．扩展频谱（Spread Spectrum，SS）局域网。

大多数无线局域网都使用扩展频谱技术（简称“扩频技术”）来传输数据。

在扩展频谱方式中，数据基带信号的频谱被扩展到几倍到几十倍，再被搬移到射频发射出去。这一做法虽然牺牲了频带带宽，却提高了通信系统的抗干扰能力和安全性。由于

单位频带内的功率降低，对其他电子设备的干扰也就减小了。

扩频技术是一种宽带无线通过技术，最早应用于军事通信领域。在扩频通信方式下，传输信息的信号带宽远大于信息本身的带宽，信息带宽的扩展是通过编码方式实现的，与所传输数据无关。扩频通信具有抗干扰能力强、隐蔽性强、保密性好、多址通信能力强等特点，能够保证数据在无线传输中完整可靠，并确保同时在不同频段传输的数据不会互相干扰。

iii．窄带微波（Narrowband Microwave）局域网。

在窄带微波局域网中，数据基带信号的频谱不做任何扩展即被直接搬移到射频发射出去。与扩展频谱方式相比，窄带调制方式占用频带少，频带利用率高。采用窄带调制方式的无线局域网一般采用专用频段，需要经过国家无线电管理部门的许可方能使用。当然，也可选用 ISM 频段，这样可免去向无线电管理委员会申请，但带来的问题是，当邻近的仪器设备也在使用这一频段时，会严重影响通信质量，通信的可靠性无法得到保证。

2）数据的传输。

当把数据传送到一个近距离的设备时，可以通过网络连接进行同步输出到远程的接收设备。而且，在传送过程中能同时传输整个字节（8 位）的数据，或是多个字节，这样就可以将整个传输速度大幅度提升。但是，对于远距离的传输则可能会因为传送信号被干扰，导致不能同时传送多个字节。

接收方必须对所收到的数据进行 Error Checking（侦错）操作，以确保传输数据的正确性。若发现收到的数据中有不符合侦错算法的内容，那么就会使用一定的措施来修复该错误，例如要求发送方重新发送被侦察到的错误位或字节。

对于无线局域网来说，因为其技术跟有线局域网是相似的，所以在每次接收通信前都会有三次“握手”的过程。这三次“握手”可以保证传送数据的双方能在可靠的连接下进行通信。

i．握手（Handshaking）。

在传送数据前，发送方并不会立即把数据传送到网络上。因为发送方并不清楚接收方是否能立即处理数据。所以为了避免发送过去的数据被接收方“置之不理”，会先发送一个要求同步的 handshaking requeests（握手要求）。

当接收方收到这样的要求，而且接收方也有足够的资源接收时，就会返回响应要求的数据包。在发送和接收双方之间经过三次“握手”操作后，就能确立一条持续通信的网络连接，如图 4-27 所示。

ii．寻找目的地（Finding the Destination）。

通常一个连接需要建立时，首先要确认该连接是连通的（即使是发送/接收双方之间有路由器等设备，把双方分割的两个不同子网络之间连接也算在该范围之内）。但由于 Wi-Fi 是利用无线电波传送数据，所以在建立无线网络时并不需要有直接的设备连接。



图 4-27　三次握手

在传输介质能连接后，设备就一直处于连接状态，直到设备被断开电源。但是该状态的连接并没有附带任何实际应用可以用到的信息，例如 IP 地址、路由信息等内容。所以，需要利用操作系统为这些连接进行初次系统级别的连接操作——handshaking。

虽然在许多连接种类中，大部分都能传送高品质的语音或者具有简单的数据传输功能。但是，对于大规模数字数据的传输则显得有点力不从心。这是因为这些连接所使用的是连接不断的通信，一旦在传输数据过程中连接收到干扰，那么所传送的大规模的数据就会发生错误。

为了传送大规模数字数据，就要把数据分成一块块的、空间占用比较小的数据，也就是所谓的 packets（数据包）。这些 packets 是从一个数据信息中切割出来的，并且通过系统封装为 packets。所谓的封装，就是把切割出来的数据整合到网络传输格式中去。所封装的 packets 会包含许多信息，例如数据的目的地、内容的大小等。

每一个数据包中都会包含目的地的 IP 地址以及邻近的序列号，这样在发送过程中就会根据序列号侦测没有到达目的地的数据包，并且根据该号码重新组合为信息。

无线网络传送包要经过切割信息、封装（把目的地的 IP 地址封装到包）、发送到目的地、解开数据包、重组信息的步骤，而这些传送操作，对于用户而言，却不会感觉到烦琐。

3）802.11b 传输控制。

因为一个网络架构须要不同的传输设备进行相互操作，所以就需要统一相互之间的传输标准，使得传输能在相互都“了解”的情况下进行，避免不同厂商所生产的网络设备发生兼容性问题。

i．物理层（The Physical Layer）。

物理层规范网络设备如何利用电子信号进行传输，并在设备之间进行协调。例如设备使用的电压，发送无线电的频率，甚至是设备与设备之间连接的线材插头都要规范为统一的形状。否则，将会因电压过高而出现烧毁设备、发射频率不同步而不能接收信号，频道与频道之间的过分接近导致干扰、线材插头不统一造成无法连接等情况。

综合来说，物理层是让不同厂商所生产的网络设备都能在统一的规范中相互传送的最

基本的数据单元，也就是常说的“0”和“1”，例如所有设备都是使用大于 3.3V 的电压表示“1”，而小于 0V 的电压则表示为“0”。

在 Wi-Fi 中同样需要统一的物理层进行规范。但有点不同的是，Wi-Fi 会在包中增加 144bits 的内容。其中，128bits 是让发送端设备以及接收端设备进行同步的内容。另外，166bits 则是一个名为 start-of-frame 的 field（字段），表示该 Frame 的开始点。

ii．访问控制层（They MAC Layer）。

MAC 层是用来控制数据从无线电波发送以及其他无线网络的产生，例如通过 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance，载波侦听多重访问/避免冲突）来解决传送冲突，或者是增加安全，使得传输更加保密。

在 Wi-Fi 中，使用的两种过滤方式分别为：SSID 以及 MAC。

其中，SSID（Service Set Identifier ，服务区域识别串）是指在 AP 的覆盖范围中的所有计算机都需要设为同一个 SSID（该 ID 必须与 AP 一致）。当客户端计算机要求进入该 AP 管辖的网络时，AP 就会检查客户端发送来的 ID 是否与自己所拥有的一致。若 ID 一致，AP 才允许计算机连接到网络；若 ID 不一致，AP 将会拒绝客户端连接到网络。而 MAC 则是利用无线上 MAC 地址（独一无二的网卡卡号）判别计算机能否能连接到网络中。

而 MAC 则通常在用户群比较固定的环境中使用，例如公司的办公室。因为，在办公室的环境中可以比较容易获得网卡上的 MAC，而且 MAC 并不会经常变化，所以在固定用户群体的环境中，使用 MAC 方式是比较常见的。

iii．其他控制层（Other Control Layers）。

除了前面所描述的物理层以及访问控制层外，还有一些在这两层之上的控制层。这些层控制许多功能，例如 IP 分配、路由、检测数据完整性等。

这些高层与其他类型的网络没有什么两样，包括光纤、无线电波等连接方式。而且，在高层上完成的网络协议也可以使用相同的种类，例如 TCP/IP、Novell NetWare、Apple Talk 等。

另外，在操作系统方面也不会有很大的区别，只要操作系统能提供兼容于 802.11b 标准的驱动程序、模块或者核心，操作系统就都能使用无线网络，例如 Windows、Unix、Mac OS、Linux 等操作系统都能使用 Wi-Fi。

4．Wi-Fi 的应用及未来展望

（1）Wi-Fi 技术的应用模式

基于 Wi-Fi 的组网架构，市场上出现了三种 Wi-Fi 的应用模式：第一，企业或者家庭内部接入模式，在企业内部或者家庭架设 AP，所有在覆盖范围内的 Wi-Fi 终端通过这个 AP 实现内部通信，或者通过 AP 作为宽带接入出口链接到互联网，这是最普及的应用方式，这时 Wi-Fi 提供的就是网络接入功能；第二，电信运营商提供的无线宽带接入服务，通过运营商在很多宾馆、机场等公众服务场所纷纷架设 AP，为公众用户提供 Wi-Fi 接入服务；

第三，“无线城市”的综合服务，基本是由市政府全部或部分投资建设，是一种类似于城市基础建设的一种模式。

1）掌上移动终端的应用。

Wi-Fi 技术最让人耳熟能详也是最主要的应用莫过于掌上移动终端的应用。如智能手机，又如苹果的 iPad，itouch 等系列产品。

近两年，市场上支持 UMA（Unlicensed Mobile Access 非授权移动接入）等技术，具备 WLAN 连接功能的智能手机越来越多。它们除了可以借助 GSM/CDMA 移动通信网络通话外，还能在 Wi-Fi 无线局域网覆盖的区域内共享计算机上网或 VoIP 通话。

Wi-Fi 手机通过无线路由器共享上网非常方便，多数 Wi-Fi 手机不需要做任何设置，在无线路由器的信号覆盖范围内，在 Wi-Fi 手机和无线路由器的默认设置下，Wi-Fi 手机就能自动获取 IP 地址进行无线连接，并利用手机自带的 IE、MSN 等软件无线上网。当然，如果在 Wi-Fi 手机和无线路由器都正常开启的情况下，Wi-Fi 手机无法通过无线路由器共享上网，我们就需要检查一下设备的设置。而 iPad，iTouch 等设备，也大体与此类似。

2）其他方面的应用。

Wi-Fi 技术就目前来看多数还是在手持掌上终端上被应用。除了能支持手机和其他掌上移动终端的各种功能外，Wi-Fi 技术还能用于导航等其他有利于人们生活的方面。例如，可以利用 Wi-Fi 的技术，制造出高增益的全向天线，比以往的天线有更大的作用。现在 Wi-Fi 技术还处在一个发展的阶段，所以很多功能还不能完全比拟现有的成熟技术，但是相信随着 Wi-Fi 的发展，这一天终将到来。

（2）Wi-Fi 的未来

1）Wi-Fi 的市场前景。

Wi-Fi 的规模商业化应用，在世界范围内罕见成功先例。问题集中在两个方面：一是大型运营商对这一模式的不认可；二是本身缺乏有效的商业模式。基于 Wi-Fi 技术的无线局域网已经日趋普及，这将意味它在将来可以十分方便地被应用。一旦存在 Wi-Fi 网络的公众场合解决了运营商的互联互通、高收费、漫游性的问题，Wi-Fi 将从一个成功的技术转化为成功的商业。诸多运营商先后涉足这一领域，且许多国家政府和城市使用该项技术打造无线化的国家和城市。随着数码娱乐设备的普及，Wi-Fi 在玩家中的热度再次高起来。据 D-link 等厂商提供的信息显示，在过去一年内，无线路由器的销量以 100%的幅度增长。

对于公共无线局域网，在欧洲，仅 BT 最近宣布已在全英建设了 50 多万个热区，在美国 ATT 继续发力 Wi-Fi 市场，通过欧洲大部分地区及中国新部署 25000 个 Wi-Fi 热区，意欲为那些商业先行者、远程工作的员工和移动用户提供更方便、更广泛的 Wi-Fi 接入，这样一来，ATT 在全球范围的 Wi-Fi 热区总数将达到 12.5 万个。

2）Wi-Fi 技术的未来发展。

Wi-Fi 是目前无线接入的主流标准，但是，Wi-Fi 会走多远呢？在 Intel 的强力支持下，Wi-Fi 已经有了接班人。它就是全面兼容现有 Wi-Fi 的 WiMAX，对比于 Wi-Fi 的 802.11X 标准，WiMAX 的标准就是 802.16x。与前者相比，WiMAX 具有更远的传输距离、更宽的频段选择以及更高的接入速度等，预计会在未来几年间成为无线网络的一个主流标准，Intel 计划将来采用该标准来建设无线广域网络。这相比于现在的无线局域网或城域网，是质的变革，而且现有设备仍能得到支持，保护人们的每一分投资。

总而言之，家庭和小型办公网络用户对移动连接的需求是无线局域网市场增长的动力，虽然到目前为止，美国、日本等发达国家仍然是 Wi-Fi 用户最多的地区，但随着电子商务和移动办公的进一步普及，廉价的 Wi-Fi 必将成为那些随时需要进行网络连接的用户的不二之选。

最近，业界纷纷传出 Wi-Fi 已出现生存危机的消息。据国外媒体报道，日前很多企业仍然在 Wi-Fi 这方面投入巨资，但从中盈利的企业几乎没有。据悉很多企业因 Wi-Fi 而破产，前不久 R Wireless 公司也放弃了该项业务。那么 Wi-Fi 的盈利情况是否真的出现危机了？

不可否认，Wi-Fi 技术的商用目前碰到了许多困难。一方面是受制于 Wi-Fi 技术自身的限制，比如其漫游性、安全性和如何计费等都还没有得到妥善的解决。另一方面，由于 Wi-Fi 的盈利模式不明确，如果将 Wi-Fi 作为单一网络来经营，商业用户的不足会使网络建设的投资收益比较低，因此也影响了电信运营商的积极性。但从 Wi-Fi 技术定位看，笔者认为，对于电信运营商而言，Wi-Fi 技术的定位主要是作为高速有线接入技术的补充，将来逐渐也会成为蜂窝移动通信的补充。

虽然 Wi-Fi 技术的商用在目前碰到了一些困难，同时这种先进的技术也不可能包办所有功能的通信系统，可以说只有各种接入手段相互补充使用才能带来经济性、可靠性和有效性。因此，Wi-Fi 技术可以在特定的区域和范围内发挥对 3G 的重要补充作用，Wi-Fi 术与 3G 技术相结合将具有广阔的发展前景。

4.5.3 蓝牙技术

1. 蓝牙技术的起源和蓝牙技术发展的各个阶段

蓝牙以公元 10 世纪统一丹麦和瑞典的一位斯堪的纳维亚国王的名字命名。它孕育着颇为神奇的前景：对手机而言，与耳机之间不再需要连线；对计算机，主机与键盘、显示器和打印机之间可以摆脱纷乱的连线；在更大范围内，电冰箱、微波炉和其他家用电器可以与计算机网络的连接，实现智能化操作。

发明蓝牙技术的是瑞典电信巨人爱立信公司。由于这种技术具有十分可喜的应用前景，

1998 年 5 月，五家世界顶级通信/计算机公司：爱立信、诺基亚、东芝、IBM 和英特尔经过磋商，联合成立了蓝牙共同利益集团（Bluetooth SIG），目的是加速其开发、推广和应用。此项无线通信技术公布后，便迅速得到了包括摩托罗拉、3Com、朗讯、康柏、西门子等一大批公司的一致拥护，至今加盟蓝牙 SIG 的公司已达到 2000 多个，其中包括许多世界最著名的计算机、通信以及消费电子产品领域的企业，甚至还有汽车与照相机的制造商和生产厂家。一项公开的技术规范能够得到工业界如此广泛的关注和支持，这说明基于此项蓝牙技术的产品将具有广阔的应用前景和巨大的潜在市场。蓝牙共同利益集团现已改称为蓝牙推广集团。

所谓蓝牙（Bluetooth）技术，实际上是一种短距离无线电技术，利用“蓝牙”技术，能够有效地简化掌上电脑、笔记本电脑和手机等移动通信终端设备之间的通信，也能够成功地简化以上这些设备与因特网之间的通信，从而使这些现代通信设备与因特网之间的数据传输变得更加迅速高效，为无线通信拓宽道路。说得通俗一点，就是蓝牙技术使得现代一些轻易携带的移动通信设备和电脑设备，不必借助电缆就能联网，并且能够实现无线上网，其实际应用范围还可以拓展到各种家电产品、消费电子产品和汽车等信息家电，组成一个巨大的无线通信网络。“蓝牙”技术属于一种短距离、低成本的无线连接技术，是一种能够实现语音和数据无线传输的开放性方案，因此，目前无线通信的“蓝牙”刚刚露出一点儿芽尖，却已经引起了全球通信业界和广大用户的密切关注。

蓝牙的支持者很多，从最初只有五家企业发起的蓝牙特别兴趣小组发展到现在已拥有了近 3000 个企业成员。根据计划，蓝牙从实验室进入市场经过了三个阶段。

第一阶段：蓝牙产品作为附件应用于移动性较大的高端产品中。如移动电话耳机、笔记本电脑插卡或 PC 卡等，或应用于特殊要求或特殊场合，这种场合只要求性能和功能，而对价格不太敏感，这一阶段的时间大约在 2001 年年底到 2002 年年底。

第二阶段：蓝牙产品嵌入中高档产品中，如 PDA、移动电话、PC、笔记本电脑等。蓝牙的价格进一步下降，其芯片价格在 10 美元左右，而有关的测试和认证工作初步完善。这一时间段是 2002—2005 年。

第三阶段：2005 年以后，蓝牙进入家用电器、数码相机及其他各种电子产品中，蓝牙网络随处可见，蓝牙应用开始普及，蓝牙产品的价格在 2～5 美元之间，每人都可能拥有 2～3 个蓝牙产品。

就目前而言，蓝牙产品的市场化正处于第三阶段的起步期。2006 年年底，蓝牙有超过 10 亿的无线用户，其中包括 5 亿多使用无线互联网访问服务的用户。第三代移动通信技术将为蓝牙互联提供更大的市场，蓝牙互联技术允许手机、便携设备、个人电脑、笔记本电脑和第三方的接入设备互相连接在一起。安装蓝牙模块的设备将从 2001 年的不足 100 万台增加到 2006 年的 16 亿台。

2. 蓝牙技术特点

蓝牙技术是一种支持设备在短距离通信的无线通信技术，能在包括移动电话、PDA、无线耳机、便携式计算机、相关外设等众多设备之间进行无线信息交换。利用“蓝牙”技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与 Internet 之间的通信，从而使数据传输变得更加迅速高效，为无线通信拓宽了道路。蓝牙采用分布式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段，数据传输速率为 1Mbps，采用时分双工传输方案实现全双工传输。

蓝牙技术是一个开放性、短距离无线通信的标准，它可以用来在较短距离内取代目前多种电缆连接方案，通过统一的短距离无线链路在各种数字设备之间实现方便、快捷、灵活、安全、低成本、小功耗的语音和数据通信。

蓝牙技术系统参数和技术指标详见表 4-2。

表 4-2　蓝牙技术的系统参数和技术指标

系统参数和技术指标	说　　明
工作频段	ISM 频段、2.402～2.408GHz
双工方式	全双工、时分双工（TDD）
业务类型	支持电路交换和分组交换业务
数据传输速率（Mbps）	1
异步信道速率（Kbps）	21/57.6（非对称连接），432.6（对称连接）
同步信道速率（Kbps）	64
功率/Mw	美国为 1（FCC 要求<0dBm），其他国家为 100
跳频频率数	79 个频点/1MHz
跳频速率/Hz	1600
工作模式	PAPK/HOLO/SNFF/ACTIVE
数据连接方式	SCO、ACT
纠错方式	1/3FEC、2/3FEC、ARQ
认证	竞争—应答方式
信道加密	0bit、40bit、60bit 密钥
语音编码方式	CSVD
发射距离/m	10～100

蓝牙产品采用低能耗无线电通信技术来实现语音、数据和视频传输，其传输速率最高为 1Mbps，以时分方式进行全双工通信，通信距离为 10m 左右，配置功率放大器可以使通信距离进一步增加。

蓝牙产品采用跳频技术，能够抗信号衰落；采用快跳频和短分组技术，能够有效地减少同频干扰，提高通信的安全性；采用前向纠错编码技术，以便在远距离通信时减少随机噪声的干扰；采用 2.4GHz ISM 频段，以省去申请专用许可证的麻烦；采用 FM 调制方式，使设备变得更为简单可靠。蓝牙技术产品一个跳频频率发送一个同步分组，一个分组占用一个时隙（也可以增至 5 个时隙）。蓝牙技术支持一个异步数据通道或 3 个并发的同步语音通道，也支持一个同时传送异步数据和同步语音的通道。蓝牙的每个语音通道支持 64Kbps 的同步语音，异步信道支持的最大速率为 721Kbps、反向应答速率为 57.6Kbps 的非对称连接，或者 432.6Kbps 的对称连接。蓝牙技术产品与 Internet 之间的通信使家庭和办公室的设备不需要电缆就能够实现互通互联，从而大大提高办公和通信效率。

3. 蓝牙协议

蓝牙协议体系中的协议按特别兴趣小组（SIG）的关注程度分为四层：核心协议，包括基带（BB）协议、链路管理协议（LMP）、逻辑链路控制适配协议（L2CAP）、服务发现协议（SDP）；串口仿真协议（RFCOMM）；电话控制协议（TCS）；选用协议，包括点对点协议（PPP）、网际协议（IP）、传输控制协议（TCP）、用户数据包协议（UDP）、对象交换协议（OBEX）和无线应用协议（WAP）、电子名片（vCard）和电子日历（vCal）。除上述协议层外，规范还定义了主机控制器接口（Host Controller Interface，HCl），它为基带控制器、连接管理器、硬件状态和控制寄存器提供命令接口。蓝牙核心协议由 SIG 制定的蓝牙专用协议组成，绝大部分蓝牙设备都需要核心协议，而其他协议则根据应用的需要而定。总之，电缆替代协议、电话控制协议和被采用的协议在核心协议基础上构成了面向应用的协议。

4. 蓝牙技术的优点

蓝牙技术提供低成本、近距离的无线通信，构成固定于移动设备通信环境中的个人网络，使得近距离内各种设备能够实现无缝资源共享。显然，这种通信技术与传统的通信模式有明显的区别，它的初衷是希望以相同成本和安全性实现一般电缆的功能，从而使移动用户摆脱电缆束缚。这决定了蓝牙技术具备以下技术特性：

1）能传送语音和数据；

2）连接性、抗干扰性和稳定性；

3）低成本、低功耗和低辐射；

4）安全性；

5）网络特性。

5. 蓝牙技术的应用

（1）蓝牙技术在外围设备的应用

蓝牙技术的主要市场是低端无线联网领域，提供简单方便的无线联网技术是业内最初

研发“蓝牙”标准的初衷。

蓝牙技术是作为一种“电缆替代”的技术提出来的，发展到今天已经演化成了一种个人信息网络的技术。它将内嵌蓝牙芯片的设备互连起来，提供话音和数据的接入服务，实现信息的自动交换和处理。

蓝牙主要针对三大类的应用：话音/数据的接入，外围设备互连和个人局域网。话音/数据的接入是将一台计算设备通过安全的无线链路连接到一个通信设备，完成与广域通信网络的互联。外围设备互连是指将各种外设通过蓝牙链路连接到主机。个人局域网的主要应用是个人网络和信息的共享和交换。

蓝牙技术已获得了 2000 余家企业的响应，从而拥有了巨大的开发和生产能力。蓝牙已拥有了很高的知名度，消费者对这一技术也很有兴趣。

在2000年，爱立信公司和ARM公司达成协议，前者将有权使用后者生产的Arm 7 RISC芯片集。作为瑞典通信领域巨头，爱立信公司打算把这种芯片应用于未来的蓝牙 PAN 技术。

爱立信微电子领域专管 Datacom 集成电路（IC）领域的总经理 Johan Tingsborg 先生指出，蓝牙和面向家庭的快速网络接入已经变成他们公司的首要应用。他说：“ARM 的处理技术将为芯片的低功率系统技术提供一个高效率的并且有明确标准的平台。”实际上，取得 ARM 的生产许可证将会极大缩短下一代通信产品投放市场的时间。

就在爱立信和 ARM 合作之前不久，Cahners In-Stat 公司提出的一份报告预测到 2005 年全世界支持蓝牙技术的设备数量将会超过 10 亿。

从芯片来看，芯片价格持续下降。英国 CSR 生产的主要蓝牙芯片产品，目前已降至 3 美元左右。芯片越来越小巧。蓝牙的技术界面是专用半导体集成电路芯片，用于嵌入电子器件内。而与用户直接见面的产品界面则是各种时尚电子产品。因此，蓝牙技术要嵌入到电子器件内就要考虑蓝牙的芯片尺寸，它必须具有小巧、廉价、结构紧凑和功能强大的特点才能放进蜂窝电话中。向单芯片方向发展，目前已经有所突破，法国 Alcatel Microelectronics 等公司在 ISSCC2001 上发表了用于蓝牙的单芯片 LSI，CSR 公司也推出了嵌入电池中的单芯片蓝牙 IC BlueCore01，产品具有兼容性。目前的产品一致性测试都已通过，但无法互通，蓝牙只有成为无线通信的“世界语”才有意义。SIG 已召集制造商召开了两次会议来测试各自蓝牙产品基础组件间的兼容情况，测试中发现的不兼问题正在解决之中。

蓝牙只是 WLAN 中的重要技术，有其局限性，WLAN 网的实现需要几种技术的结合。众多操作系统支持蓝牙。微软公司于 2001 年上市的 Windows 操作系统——Whistler 也支持蓝牙。以 IBM 为首的众多计算机厂商正在努力达成协议，为 PC 平台制定蓝牙标准，以解决不同设备之间的兼容性。美国 Mobilian 公司推出了兼具无线 LAN 和 Bluetooth 功能的芯片组。这个由两个芯片构成的芯片组具备无线 LAN 的标准方式——IEEE 802.11b 的无线收发功能和蓝牙功能。由于 IEEE 802.11b 和蓝牙的载波频带都使用 2.4GHz 频带，当同时收

发这两种规格的数据时，有可能引起数据包冲突等电波干扰，一直无法同时应用。Mobilian 公司此次开发的芯片组中，通过采用消除电波干扰的方法，实现了两种规格数据通信同时进行。蓝牙技术可以在微网络或扩大网之间切换，但每次切换都必须断开与当前 PAN 的连接。为解决此问题，Commil 技术公司设计了一种系统，即使在蓝牙模式不同入口点之间漫游，仍可以维持连续的、不中断的数据和声音交流。这种蓝牙网络技术提供很好的连接，其中一个连接是从一个蓝牙入口点出发，在连接中保证不断开。作为一种近距离的无线通信技术，蓝牙技术并不是唯一的。但是与其他相应的无线通信技术比较起来，蓝牙技术的优势就在于它是全球统一的，开放的技术标准，具有技术先进与成本低廉，以及世界蓝牙组织 SIG 知识产权共享的巨大诱惑力。

在蓝牙技术联盟中国 2008 峰会上，蓝牙技术联盟成员展示了最新的蓝牙产品和服务。在这次峰会上，支持蓝牙功能的手机、耳机、车载免提设备、蓝牙技术测试装置和认证服务以及蓝牙遥控游戏机等相继亮相。蓝牙技术联盟亚太区及日本市场总监苏国良在会上指出：“作为蓝牙产品研发和生产的核心部分之一，中国成员公司在蓝牙技术的发展过程中扮演着至关重要的角色。未来，具有低功耗和高速传输特点的蓝牙技术将继续引领个人无线通信领域，并打开新的市场。”另外，他还补充道：“目前，蓝牙技术联盟已经在中国设立了 3 家蓝牙认证测试中心，他们将在蓝牙认证程序，尤其是蓝牙技术测试领域为中国蓝牙设备制造商提供专业的品质服务。”2008 年 7 月，蓝牙技术联盟与北京天地互联合作在北京设立了办事处，为近 600 名中国成员提供技术支持以及增值服务。这一系列举措都体现了联盟对中国市场的重视以及在中国推动蓝牙技术应用的坚定信心。北京天地互联总裁刘东在峰会上表示：“在联盟中，中国成员公司的数量在全亚洲一直排名靠前。我们将与蓝牙技术联盟一道为中国蓝牙产业的良性发展继续贡献力量。”

如今的蓝牙相关的配件已经不再是昂贵的天价，随着蓝牙技术的成熟和普及越来越多的厂商开始介入蓝牙相关附件产品的生产制造，也把价格降到了一个大众可以接受的程度。

目前国际市场上比较活跃的蓝牙设备生产商有四家，分别是 Jabra、i-Tech、Plantronics 以及 OMIZ。在这些厂商中 Jabra 和 i-Tech 很早就进入了中国市场，这两家厂商的产品也主要以蓝牙耳机、蓝牙音箱等免提音频设备为主。而 Plantronics 同样也是专注于耳麦领域的厂商，至于最后一家 OMIZ 则是一家全方位的蓝牙设备制造商。很多著名厂商的蓝牙耳机、蓝牙适配器、PDA 折叠蓝牙键盘以及蓝牙鼠标等产品都是 OMIZ 的贴牌产品。如今 OMIZ 这位我们最熟悉的陌生人即将要以自己的品牌进入中国市场，无疑是给中国蓝牙产品的市场注入了新的活力。

（2）蓝牙技术在 3G 技术中的应用

目前我们日常生活中听到过的蓝牙最为广泛的应用当属蓝牙耳机了。曾经蓝牙耳机是作为一项高科技出现在我们的视线当中的，当时带有蓝牙功能的手机也寥寥无几，而且价

格并不能为广大消费者所接受。而今，纵观手机市场，几乎 70%的手机都具有了蓝牙功能，著名的手机厂商甚至在部分低端手机上也开始加入了蓝牙功能。蓝牙已经普及到了我们的生活当中。而蓝牙耳机的价格也已经到了大众所能够消费的水准。

为什么说 3G 跟蓝牙有关呢？我们对 3G 手机最初的认识是 3G 手机有视频通话功能，而视频通话是通过手机的一个前置摄像头来实现的，那么要进行视频通话就不能够像平时一样握着手机把手机贴在脸上进行通话了，视频通话只能够通过免提耳机进行。这时候蓝牙耳机的作用就能够发挥出来了。

现在也有很多商务人士经常需要在外使用到无线上网功能。3G 时代来临后，这一应用人群势必扩大，我们现在所使用的手机几乎都带有无线调制解调器功能，所需要的只是通过数据线或是蓝牙连接到计算机便能够使用。当然数据线还需要专门的驱动程序，蓝牙就没这个麻烦了，只要用户的计算机具有蓝牙功能或者是自己安装了蓝牙适配器，那么直接跟手机配对设置就能够通过手机来无线接入 Internet，随时随地，不受任何限制。

（3）蓝牙技术在生活领域中的应用

私家车市场的成熟也是促使蓝牙发展的一个重要因素。媒体一直都在教育广大司机朋友们开车打话是非常危险的事情，而如果您使用蓝牙耳机进行通话的话便可以大大降低边打电话边开车的危险性。笔者在国外看到各种车辆的司机几乎是人手一个蓝牙耳机，国内目前也正在逐渐地形成同样的一个氛围。随着交通法规的完善，人民生活水平以及素质的提高，蓝牙耳机也会随着手机一同普及。

当然，我们现在的蓝牙应用并不仅限于免提通话，各大手机厂商和蓝牙设备厂商也开始推出用于无线音乐的立体声蓝牙耳机。随着音乐手机的普及，大家都已经放下了手中的 MP3，开始习惯了使用手机来听音乐。但是耳机线在包里绕来绕去终究是一件麻烦的事情，有了立体声蓝牙耳机，可以摆脱线的束缚，何乐而不为呢？并且蓝牙耳机还没有有线耳机的接口限制，即便是您换了新手机也可以继续使用原来的蓝牙耳机，完全不需要额外购入任何新设备。

蓝牙技术最初仅被设想为用于耳机和手机之间的数据传输，然而消费者不断变化的使用需求让蓝牙技术的应用更加多元化，逐步渗透到电子游戏、计算机备件和医疗领域。近十年来，蓝牙技术深受欢迎，至今全球已有超过 20 亿件蓝牙设备问世，蓝牙技术联盟更是由寥寥 5 名成员成长为万人大家庭，蓝牙品牌知名度提高到八成。玩游戏、听音乐、结交新朋、与朋友共享照片，越来越多的消费者希望能够方便即时地享受各种娱乐活动，而又不想再忍受电线的束缚。Bluetooth 无线技术是唯一一种能够真正实现无线娱乐的技术。内置了 Bluetooth 技术的游戏设备，让您能够在任何地方与朋友展开游戏竞技。在地下通道、在飞机场或在起居室中。由于不需任何电线，玩家能够轻松地发现对方，甚至可以匿名查找，然后开始令人愉快的游戏。

Bluetooth 无线技术使发送照片到打印机或朋友的手机也变得非常简单。现在，很多商店提供打印站服务，让消费者能够通过 Bluetooth 连接打印拍照手机上的照片。

娱乐不再局限于设备的线长范围内。不管是骑自行车、徒步旅行、滑雪还是旅行，Bluetooth 技术都扩大了业余活动的活动范围，带来真正的无线体验。制造商目前能使用 Bluetooth 技术将 MP3 播放器手机连接到内置了立体声耳机的滑雪头盔和帽子上。

在山上，通过 Bluetooth 连接将 GPS 设备链接到 PDA 上，就能知道您身在何处。地理寻宝和徒步旅行爱好者期待着采用最新 Bluetooth 的设备来帮助他们确定路线和跟踪行程。

不管是在等待公共汽车还是乘坐火车，您都可以使用 Bluetooth 技术打发时间。对于装有游戏的设备，可搜索启用类似设置的设备来进行多人游戏。使用在 Bluetooth 电话上运行的软件应用程序，查找您身边有相同兴趣的其他人，或只是用于识别那些您在日常路线上遇到的 Bluetooth 设备。看看那些经常与您擦身而过的“熟悉的陌生人”。通过 Bluetooth 技术，向启用类似设置的手机发送消息，结交新朋友。

6. 蓝牙技术对未来的影响

蓝牙无线接入技术如主干网络的神经末梢将通信技术渗透到各行各业。蓝牙无线通信技术的出现之所以引起企业界如此广泛的关注，就是因为它为其他领域的技术发展注入了鲜活的生命力。例如，瑞典 ABB 公司将蓝牙技术、网络技术及智能技术相结合应用在工业环境中。

蓝牙无线技术对我国的信息化建设来说，既是挑战也是机遇。我们衷心希望具有我国自主知识产权的蓝牙产品早日投入市场，也希望有更多的有识之士关注和支持我国蓝牙技术的成长与发展，也许在不久的将来，人们会惊奇地发现我们的工作与生活都在逐步变“蓝”。

作为一种短距离无线通信技术，蓝牙可以将通信、个人电脑、网络、工业、自动化和家用电器等通过语音或数据连接在一起，距离可以达到 10m，甚至 100m。蓝牙技术的优势就在于它使用户从纷繁复杂的连线中解放出来，商家和客户可以更简单灵活地实现同步通信，同时也更有利于在同事、朋友或办公网络中建立更快速便捷的联络。就蓝牙技术而言，尽管支持蓝牙技术的移动设备比较简单，但它们都要连接到蓝牙中央服务系统上，这套服务系统的运作方式就像家庭或办公室中的集线器（HUB）。正因为如此，爱立信公司准备将 ARM 公司的 RISC 处理器技术在这种集线器中使用，他们预测蓝牙技术非常有希望成为未来多种多样 IT 系统的标准。爱立信公司和 ARM 公司达成协议，前者将有权使用后者生产的 Arm 7 RISC 芯片集。作为瑞典通信领域巨头，爱立信公司打算把这种芯片应用于未来的蓝牙 PAN 技术。

蓝牙技术发展迅速，应用广泛，市场前景良好，但蓝牙技术目前的现状，特别从 2003 年的蓝牙世界大会所暴露的问题来看，前景仍然不容乐观。虽然目前蓝牙技术在业界受到广泛的关注，但是仍未获得消费者的足够认可。在进行蓝牙产品的销售过程中，没有很好

地为消费者解释为什么要使用蓝牙技术，因为消费者只想使用可行的无线技术，而并不是过分关心它的类别。目前蓝牙技术 1.0 的标准还只能传输 1Mbps 的语音和数据，但是 2003 年推出的蓝牙技术 2.0 标准的传输速率可达到 12Mbps，它还将采用智能跳频技术与 1.0 的标准兼容。购买了蓝牙设备的顾客首先要花几个小时的时间来研究菜单、配对蓝牙设备和设置规则，然后才能连接两个蓝牙系统，使用起来极不方便。互操作性是所有通信设备的重要特性，蓝牙产品也不例外。从理论上说只要通过了产品的一致性和互连性测试，互操作性问题就可以得到解决。在目前充满竞争的无线标准市场，要指明蓝牙的未来并不是一件容易的事。一方面，蓝牙技术需要不断改进，以适应医疗电子、工业控制和家电自动化领域的潜在应用；另一方面，许多人警告，随着数据率的增高，蓝牙的市场定位更变得令人困惑。

一项新技术的出现，人们对它抱的期望值往往很高，短期内往往不能令人满意，这是因为任何新技术的发展都需要有一个过程，蓝牙技术也不例外；技术标准统一，知识产权共享的优势是非常明显的，相信通过业界的共同努力，蓝牙技术未来的发展是不可限量的，从长远来看可能会超出人们的想象。

第 5 章　物联网与传感网中故障诊断、容错、修复与安全

5.1　物联网与传感网常见故障类别

5.1.1　传感器网络故障原因

在传感器网络中，传感器结点具有端结点和路由的功能。一方面实现数据的采集和处理；另一方面实现数据的融合和路由，对本身采集的数据和收到的其他结点发送的数据进行综合，转发路由到网关结点。网关结点往往个数有限，而且能量能够经常得到补充。网关通常使用多种方式（如 Internet、卫星或移动通信网络等）与外界通信。而传感器结点数目非常庞大，通常采用不能补充的电池提供能量，传感器结点的能量一旦耗尽该结点就不能进行数据采集和路由的功能，直接影响整个传感器网络的健壮性和生命周期。因此，传感器网络主要研究的是传感器网络结点。实际应用过程中，传感器结点也是最容易出现故障的环节。传感器在工作过程中常遇到的问题有：

1）测量环境中存在空间辐射干扰、信号通道或电源干扰等，引起测量误差；

2）传感器的增益突然衰减或使用一段时间后逐渐衰减以至产生测量误差；

3）传感器输出出现超阶跃型偏差或缓变型偏差等。

由于干扰、增益、偏差等原因引起的测量误差其幅度范围有可能和系统真实故障引起的幅度偏差范围相同，如果未对传感器的输出信号进行处理判断就对监测系统实施故障诊断，很有可能出现漏判或误判。因此，及时发现传感器自身故障尤为重要，有必要建立传感器故障实时监测系统。

与有线信道的传输相比，无线信道的传输更容易发生故障。信号波形的反射、衍射和散射之类的现象及结点的运动都会导致快衰落和码间干扰的发生。路径损耗、衰减和障碍

物的存在均会导致慢衰落的发生。此外，来自其他结点或其他系统的噪声和干扰如果处于相同或相邻的频段，也会对其系统造成影响。波形失真也可以引起比特差错和分组丢失，从而产生网络故障。

5.1.2 传感器网络故障分类

网络故障以某种症状表现出来，故障症状包括一般性的（用户不能接入某个服务器）和较特殊的（如路由器不在路由表中）。对每一个症状使用特定的故障诊断工具和方法都能查找出一个或多个故障原因。

采用从系统级的角度进行故障诊断，其故障相应地分为能量供应模块故障、传感器模块故障、CPU 模块故障和无线通信模块故障四类。

另外，故障根据性质可分为硬故障和软故障。硬故障结点可以被其他结点感知，但不能和其他结点进行通信（例如通信软硬件发生故障或能量不足的移动结点）；软故障结点虽然发生故障，但仍可以继续工作并与其他结点进行通信，但工作状态不正常（例如通信相关的软硬件都正常，但是移动结点上层应用出现故障）。

故障检测是故障定位和修复的前提，主要包括数据故障检测、网络故障检测和软件故障检测三类。

（1）数据故障检测

作为数据型网络，感知数据的正确性对传感器网络的应用尤为重要。为了获取物理世界信息，传感器网络通常被部署在无人看护的户外或者环境较为恶劣的区域，这使得感知数据质量很容易受到部署环境的影响。如果传感器上报数据与实际物理现象不一致，我们则认为发生了数据故障。硬件故障、连接失效、校准参数的漂移、环境噪声以及软件缺陷都会导致数据故障。故障数据的处理和传输会浪费系统资源，更重要的是大量故障数据会导致应用本身无法正常工作。数据本身的属性（如最大值、最小值和变化率等）以及多个数据点在时空上的约束关系（如同一时刻相邻位置或者同一位置相邻时刻的温度具有相关性）是数据故障检测的主要依据。

（2）软件故障检测

传感器网络中很大一部分故障与软件缺陷有关，如果能在软件层面尽早检测出故障，则会减少后期故障定位的难度。因此有效的软件故障检测技术可以在很大程度上解决传感器网络故障定位问题。

1）基于测试的故障检测。

测试是系统部署前故障检测的主要手段，测试环境的相对可控性使部署前的故障检测较部署后更为容易。然而，测试环境与实际部署环境的差异以及现有测试方法在应用于传感器网络测试时的各种不足，很大程度上降低了部署前测试对软件故障检测的有效性。针

对这一问题，基于测试的故障检测一方面需要尽可能减小测试环境与部署环境的差异，另一方面需要根据传感器网络特点对传统测试方法进行改进。

2）运行时故障检测。

传感器网络与物理世界紧密耦合的特点使得部署前的测试仅能对实际部署后系统的正确性和各项性能参数做出一个大致评估。而那些部署后出现的问题常常无法在部署前测试中发现。部署后故障需要使用运行时故障检测技术进行检测。程序运行时故障检测是根据程序运行时的状态，对故障进行自动识别的过程。资源上的限制使传感器网络具有非常有限的可见性，而部署环境的复杂与不可控性又使故障再现十分困难，这些都给部署后的故障检测与定位带来了巨大的挑战。有效运行时故障检测可以使传感器网络具有 fail-fast 属性，具有这种属性的系统能在故障发生后尽可能早地捕获故障，并向用户提供与引发故障最为相关的系统状态信息，从而帮助用户更加容易和快速地对故障进行定位。

5.2　物联网与传感网常见故障诊断

故障诊断技术是一门综合性技术，其研究涉及多门学科，如电子计算机理论与技术、自动控制技术、信号处理技术、仿真技术、数理统计模糊集理论、信息处理模式识别人工智能等应用型的多学科交叉的边缘学科。近年来，故障诊断技术发展迅速，在交通运输、武器装备、航空航天、医学研究、发电设备、机器人及其他工业自动化领域得到了广泛的应用，取得了良好的经济与社会效益。

所有感知到故障的网络对象（包括物理对象和逻辑对象）都会发生告警，在一个大型网络中，一个故障可能会引起大量的告警。故障诊断就是对网络设备发出的告警进行相关处理，从一大堆的告警中找到故障发生的真正原因，并找出故障结点。在网络故障诊断中，一个理想的告警应该包含有关故障的“五 W”信息（Who、What、Where、When 和 why）。由于网络设备对于自身以外的网络情况的知识了解非常有限，所以网络设备产生的大部分网络告警只回答了 who、what 和 when 三个问题，而故障诊断要进行 where 和 why 的推理。另外，告警噪声的存在进一步增加了故障诊断的难度，这些告警噪声包含告警丢失、延迟、重复和虚假告警等。

5.2.1　故障诊断目的及性能标准

（1）故障诊断目的

故障诊断应该实现三方面的目的：确定网络的故障点，恢复网络的正常运行；发现网络规划和配置中欠佳之处，改善和优化网络的性能；观察网络的运行状况，及时预测网络

通信质量。网络故障诊断以网络原理、网络配置和网络运行的知识为基础。从故障现象出发，以网络诊断工具为手段获取诊断信息、确定网络故障点、查找问题根源、排除故障、恢复网络正常运行。诊断网络故障的过程应该沿着 OSI 七层模型从物理层开始向上进行。

（2）任务与性能标准

故障诊断的任务，由低级到高级，可分为以下几个方面的内容：故障建模（fault modeling）、故障检测（fault detection）、故障分离（fault isolation）、故障分析/识别（Fault Analysis/identification）、故障诊断（fault diagnosis）、故障的评价与决策（evaluation and decision）等。故障诊断的方式包括通过研究在一定工作环境下导致网络系统某种功能失调的原因或性质；根据系统症候，判断系统是否发生了故障；判断劣化状态发生的部位以及确定设备故障的种类；确定故障的大小以及故障发生的时间，预测状态劣化的发展趋势。

评价整个监测系统的性能指标大体上可分为以下三个方面：

1）检测性能指标（Detection Performance Index）。

早期检测的灵敏度是指一个故障检测系统对“小”故障信号的检测能力。检测系统早期检测的灵敏度越高，表明它能检测到的最小故障信号越小。

故障检测的及时性是指当诊断对象发生故障后检测系统在尽可能短的时间内检测到故障发生的能力。故障检测的及时性越好，说明从故障发生到被正确检测出来的时间间隔越短。

故障的误报率和漏报率。其中误报是指系统没有发生故障却被错误地判定为出现了故障；漏报则是指系统中出现了故障却没有被检测出来的情形。一个可靠的故障检测系统应当保持尽可能低的误报率和漏报率。

2）诊断性能指标（Diagnosis Performance Index）。

故障分离能力是指诊断系统对不同故障的区分能力。这种能力的强弱取决于对象的物理特性、故障大小、噪声干扰、建模误差以及所设计的诊断算法。分离能力越强，表明诊断系统对于不同故障的区分能力越强，对故障的判断越准确。

故障识别的准确性是指诊断系统对故障的大小及其时变特性估计的准确程度。故障识别的准确性越高，表明诊断系统对故障的估计就越准确，也就越有利于故障的评价与决策。

3）综合性能指标（Comprehensive Performance Index）。

鲁棒性是指故障诊断系统在存在噪声、干扰、建模误差的情况下正确完成故障诊断任务，同时保持满意的误报率和漏报率的能力。一个故障诊断系统的鲁棒性越强，表明它受噪声、干扰、建模误差的影响越小，其可靠性也就越高。

自适应能力是指故障诊断系统对于变化的被诊断对象具有自适应能力，并且能够充分利用由于变化产生的新信息来改善自身。引起这些变化的原因可以是被诊断对象的外部输

入的变化、结构的变化或由诸如生产数量、原材料质量等问题引起的工作条件的变化等。

上述性能指标分别从检测性能、诊断性能以及综合性能三个不同的方面给出了评判一个故障诊断系统性能的标准。在实际的工程设计中，首先要正确分析条件以及最终的性能要求，明确哪些性能是主要的，哪些是次要的，然后对众多的故障诊断方法进行分析，经过适当的权衡和取舍，最终选定最佳的解决方案。

5.2.2　故障诊断技术

故障诊断技术发展至今已经出现了基于各种不同原理的众多方法。同以往相比，这些方法不论是检测性能、诊断性能，还是鲁棒性能都有很大提高，而且对于线性不变系统已经形成了相对较为完整的体系结构。国际故障诊断权威，德国的 Frank 教授认为所有的故障诊断方法可以划分为基于知识的方法、基于解析模型的方法和基于信号处理的方法三大类，如图 5-1 所示。

5.2.3　传感器故障诊断技术

过去的十几年里，传感器故障诊断采用的方法主要是各种各样的冗余法例，主要分为三种：直接冗余、解析冗余、时序冗余。直接冗余又称硬件冗余，它采用多个传感器来测量同一个系统参数。硬件冗余法不需要被控对象的数学模型，具有较强的鲁棒性，但这种传感器硬件冗余技术要求所有参与冗余的传感器具有相同的参数特性，并且增加了设备的体积、成本。解析冗余法利用系统静动态数学模型所提供的系统不同输出量之间的解析关系产生输出量的冗余信息，不需要增加硬件设备，成本低。其主要难点在于建立精确的传感器数学模型，计算量大、鲁棒性差。系统的状态检测与故障诊断运用到了大量具有相关性的传感器组群，对与监测具有相同对象相同性质的状态参数来说，传感器组群之间具有一定的冗余性，利用冗余性，可以进行传感器的状态判别。时序冗余是用某传感器的时间序列输出得到的冗余信息来检测故障。幅值检测和变化率检测就经常用于时序冗余法的检测中。早期的传感器可靠性技术采用的主要方法是硬件冗余，通过提高传感器的质量或多传感器备份冗余，取其平均值或多选值。这种方法具有原理简单，不依赖系统的数学模型，检测速度快等优点，但是对于复杂系统，该方法将带来系统规模过分庞大，成本费用过高等弊端，所以已不适应现代工程需要。解析冗余法就避免了硬件冗余的各种缺点，它改善传感器的可靠性是以增加机载计算量为代价的，而硬件成本和重量几乎不变，因此获得了更多的应用。综合似然率、多模型卡尔曼滤波器以及最大似然率检测器等都是现有典型的解析冗余法，它们都可以实现对传感器信号的连续监测。解析冗余的缺点是需要建立系统的数学模型，这种方法对模型的可靠性和精度要求很高。系统的建模误差、未建模动态和参数时变等将对故障诊断结果产生很大的影响，因此难以应用于具有模型不确定性的系统

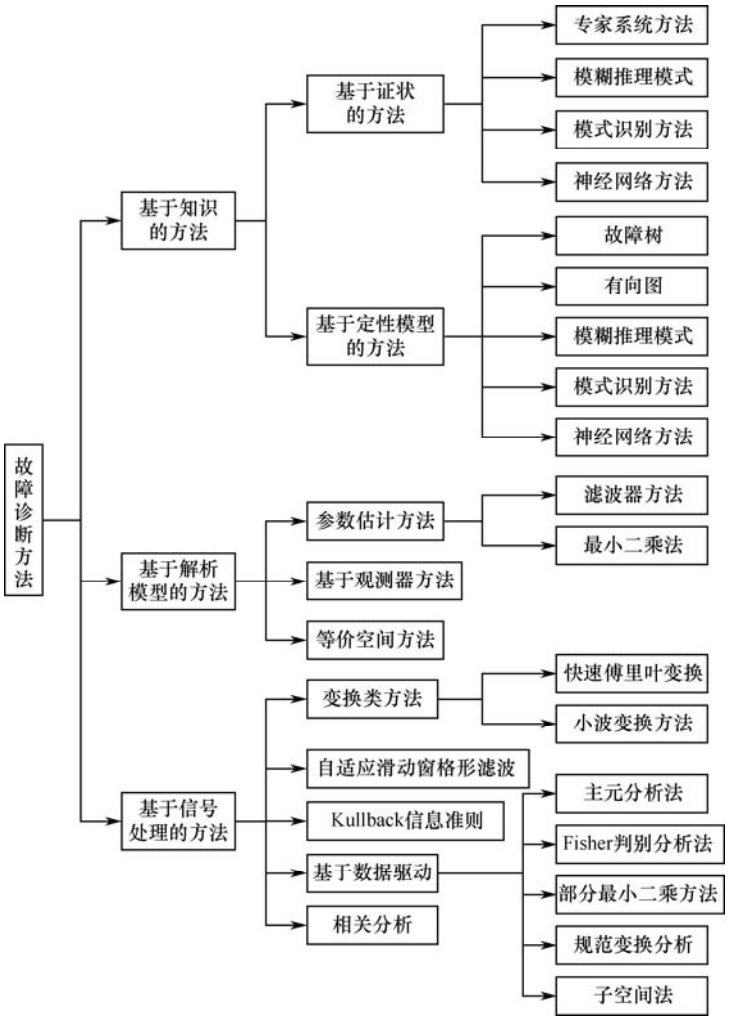


图 5-1　故障诊断方法分类示意图

和非线性系统。可见，研究不依赖于系统模型，不增加硬件冗余度，又能可靠检测传感器故障的方法是近年来传感器故障检测方法的发展方向。

传感器故障诊断本质上是一个多源信息处理过程，多传感器信息融合技术在该领域充分发挥优势，在传感器故障诊断过程中起到了重要的作用。由于多传感器信息融合分三个层次，即像素级融合、特征级融合和决策级融合，该技术在传感器故障诊断中起到的作用也体现在这三个层次上。

1）像素级融合层次上，该技术按照融合过程的 I/O 特性起到两方面的作用：

第一，I/O 特性为数据输入/数据输出时，该技术可以直接利用系统中已有的大量传感器提供的数据冗余或互补关系，借助于特定的融合算法，将各种不同的测量数据进行融合处理，能够得到对被测参数（被诊断传感器的测量信号）更全面、更准确的融合值。一方面该融合值为下一步进行有效的传感器故障诊断提供了重要的依据；另一方面，若传感器出现了故障，该融合值能够有效及时地代替出现故障的传感器信号。

第二，I/O 特性为数据输入/特征输出时，这个过程主要是将被诊断传感器自身的测量数据以及某些中间结果和系统知识进行融合，以获取有关传感器故障的各种特征信息，为传感器故障诊断提供重要依据。

2）特征级融合层次上，其 I/O 特性是特征输入/特征输出，其起到的重要作用是按照一定的目标需要对已提取的传感器故障特征在空间和时间上进行数量或质量的分析与合并。

3）决策级融合层次上，按融合过程的 I/O 特性分别起到两方面的作用：第一，特征输入/决策输出时，该过程在已知传感器故障特征的基础上，通过对来自不同信息源的故障特征进行融合识别，从中得出诊断结果，典型应用的融合方法如神经网络法、模糊识别法等。第二，决策输入/决策输出时，该过程可对各个局部的传感器故障诊断结果进行进一步的融合，通过决策规则来实现全局故障诊断，这在很大程度上降低了单一诊断信息的模糊性和不确定性，使得最终的诊断结果更加精确可靠。

5.2.4　传感器网络故障诊断技术

随着无线传感器的结构越来越复杂，功能越来越完善，自动化程度也越来越高。由于许多无法避免的因素影响，加之 WSN 使用的环境异常复杂和恶劣，WSN 的结点会出现各种故障，这会使 WSN 预定的功能降低或失去，甚至造成严重的损失乃致整个网络瘫痪。通过故障诊断能及时、正确地对各种异常状态或故障状态给出诊断、预防或消除。对传感器的运行进行必要的指导，提高传感器运行的可靠性、安全性和有效性，以及把故障损失降低到最低限度，保证 WSN 发挥最大的设计能力，可以在允许的条件下充分挖掘 WSN 的潜力，延长其使用寿命。

从研究进展来看，WSN 技术已大大超前 WSN 故障诊断的技术，因此 WSN 结点的故障诊断问题就迫在眉睫。

目前，WSN 故障研究主要分为故障检测及修复技术和故障容忍技术。其中对故障容忍技术研究较多，其主要思想是为了使结构化的分析有意义，不论通信或传输是否出现错误，在每一步测量中至少要收集到一定的数据。

5.2.5　无线传感器网络与传统 IP 网络故障诊断区别

第一，无线传感器网络最大的特点是其能量的有限性，因此，关于传感器网络的各种

设计与使用问题都不能抛开能量效率。无论是路由协议或 MAC 协议，都把能量问题放在首位，以确保整个网络长期有效地进行工作。因此，无线传感器网络的故障诊断方法设计也必须关注能量效率，这与有线网络有着根本的区别。

第二，由于不存在布线，传感器网络不用考虑物理线路方面的故障。

第三，传感器结点的工作任务主要是信息采集和传输，它注重有关物理环境的实际信息并不关心对某一结点的识别。传感器结点关注的焦点是数据而非结点识别，可以说传感器网络是以数据为中心的网络。结点既肩负着信息采集的任务，同时还要将信息传输到其他结点，这个过程中任意环节都可能出现错误。传感器网络故障诊断的目标主要是保障数据在采集、处理、传输及其使用过程中的正确性。而 IP 网络故障诊断不仅仅针对数据，更多的是对网络的连通性、通信协议的正确性以及通信质量的关注。

第四，传感器网络由于其分布的特殊性，无法直接借助人为力量对整个网络进行维护，一般的解决方案往往是采用冗余或放弃故障结点重新选择最佳路径传输数据。如果采用故障修复的方法，就会加剧结点能量的消耗，反而得不偿失。因此 WSN 更强调自组织、自维护地工作。而 IP 网络借助网络协议分析仪等设备可以更多地观察到故障的位置和类型，从而进行人工分析以处理故障、修复故障。

第五，无线传感器网络结点能量耗尽后，该结点就会被弃用，网络结构会重新调整。相对 IP 网络而言，传感器结点及传感器网络拓扑的不确定性大大增加，这就需要使用的故障诊断方法简单实用，更多的注重诊断的最终结果而不是故障分析的过程。

5.3 物联网与传感网常见纠错与修复

5.3.1 物联网与传感网故障修复的特点

故障修复是调试过程中的重要一环，其目的是对部署后的传感器网络系统及应用进行缺陷排除、功能升级和性能优化以适应周边物理环境和自身动态系统的变化。与传统故障修复相比，传感器网络故障修复除了遵循通用的原因分析、缺陷排除、复查测试和确认正常等步骤外，还具有如下特点：

（1）原地（in situ）故障修复

由于众多感知结点深度嵌入于物理环境之中，系统一旦部署，在许多应用场景下（如野生动物习性监测、深海、火山喷发口）物理接触全部结点并不现实，因此需要借助无线链路对远程结点上运行的软件缺陷进行修复。实现该过程的途径通常被称为“空中”重编程（over-the-air reprogramming）。

（2）故障修复能力与故障修复代价存在矛盾

传感器网络故障修复能力取决于空中重编程的粒度和结点执行环境能力。因为不同层次的抽象级别使对底层的完整执行程序或程序部分模块的更新比对高层虚拟机脚本的更新具有更强、更灵活的修复能力。而现有的研究已表明传感器结点传输信息要比执行计算更消耗能量，这使得想要获得更高的故障修复能力就可能产生更大的故障修复代价。

5.3.2　几种常见的威胁分析与对策

未来的传感器网络一般有成百上千个传感结点，很难对每个结点进行监控和保护，因而每个结点都是一个潜在的攻击点，都可能被攻击者进行物理和逻辑攻击。另外，传感器通常部署在无人维护的环境当中，这更加方便了攻击者捕捉传感结点。当捕捉了传感结点后，攻击者就可以通过编程接口（JTAG 接口）修改或获取传感结点中的信息或代码。根据文献分析，攻击者可利用简单的工具（计算机、UISP 自由软件）在不到一分钟的时间内就把 EEPROM、Flash 和 SRAM 中的所有信息传输到计算机中。通过汇编软件，可很方便地把获取的信息转换成汇编文件格式，从而分析出传感结点所存储的程序代码、路由协议及密钥等机密信息，同时还可以修改程序代码，并加载到传感结点中。

很显然，目前通用的传感结点具有很大的安全漏洞，攻击者通过此漏洞可方便地获取传感结点中的机密信息，修改传感结点中的程序代码。如使传感结点具有多个身份 ID，从而以多个身份在传感器网络中进行通信。另外，攻击还可以通过获取存储在传感结点中的密钥、代码等信息，伪造或伪装成合法结点加入到传感网络中。一旦控制了传感器网络中的一部分结点，攻击者就可以发动很多种攻击，如监听传感器网络中传输的信息，向传感器网络中发布假的路由信息或传送假的传感信息，进行拒绝服务攻击等。

对策：由于传感结点容易被物理操纵是传感器网络不可回避的安全问题，必须通过其他的技术方案来提高传感器网络的安全性能。如在通信前进行结点与结点的身份认证，设计新的密钥协商方案，使得即使有一小部分结点被操纵，攻击者也不能或很难从获取的结点信息推导出其他结点的密钥信息等。另外，还可以通过对传感结点软件的合法性进行认证等措施来提高结点本身的安全性能。

根据无线传播和网络部署特点，攻击者能很轻易地通过结点间的传输获得敏感或者私有的信息。例如：在通过无线传感器网络监控室内温度和灯光的场景中，部署在室外的无线接收器可以获取室内传感器发送过来的温度和灯光信息；同样攻击者通过监听室内和室外结点间信息的传输，也可以获知室内信息，从而揭露出房屋主人的生活习性。

对策：对传输信息加密可以解决窃听问题，但需要一个灵活、强健的密钥交换和治理方案。密钥治理方案必须容易部署而且适合传感结点资源有限的特点。另外，密钥治理方案还必须保证当部分结点被操纵后（这样，攻击者就可以获取存储在这个结点中的

生成会话密钥的信息），不会破坏整个网络的安全性。由于传感结点的内存资源有限，使得在传感器网络中实现大多数结点间端到端安全不切实际。然而在传感器网络中可以实现跳–跳之间的信息的加密，这样传感结点只要与邻居结点共享密钥就可以了。在这种情况下，即使攻击者捕捉了一个通信结点，也只是影响相邻结点间的安全。但当攻击者通过操纵结点发送虚假路由消息，就会影响整个网络的路由拓扑。解决这种问题的一种办法是采用具有鲁棒性的路由协议，另一种方法是采用多路径路由，通过多个路径传输部分信息，并在目的地进行重组。

传感器网络将收集信息作为主要目的，攻击者可以通过窃听、加入伪造的非法结点等方式获取这些敏感信息。假如攻击者知道从多路信息中获取有限信息的相关算法，攻击者就可以从获取的大量信息中导出有效信息。一般传感器中的私有性问题，并不是通过传感器网络去获取，而是攻击者通过远程监听 WSN，从而获得大量的信息，并根据特定算法分析出其中的私有性问题。由于攻击者并不需要物理接触传感结点，远程监听是一种低风险、匿名的获得私有信息方式。同时，远程监听还可以使单个攻击者同时获取多个结点的传输的信息。

对策：保证网络中的传感信息只有可信实体才可以访问是保证私有性问题的最好方法，这可通过数据加密和访问控制来实现。另外一种方法是限制网络所发送信息的粒度，因为信息越具体，越有可能泄露私有性。比如，一个簇结点可以通过对从相邻结点接收到的大量信息进行汇集处理，并只传送处理结果，从而达到数据匿名化。

DOS 攻击主要用于破坏网络的可用性，减少执行网络或系统某一期望功能的任何事件。如试图中断、颠覆或毁坏传感网络，另外还包括硬件失败、软件 bug、资源耗尽、环境条件等。这里我们主要考虑协议和设计层面的漏洞。确定一个或一系列错误是否由有意 DOS 攻击造成是很困难的，特别是在大规模的网络中，因为此时传感网络本身就具有比较高的单个结点失效率。

DOS 攻击可以发生在物理层，如信道阻塞，这可能包括在网络中恶意干扰网络协议的传送或者物理损害传感结点。攻击者还可以发起快速消耗传感结点能量的攻击，比如向目标结点连续发送大量无用信息，目标结点就会消耗能量处理这些信息，并把这些信息传送给其他结点。假如攻击者捕捉了传感结点，那么它还可以伪造或伪装成合法结点发起这些 DOS 攻击，比如它可以产生循环路由，从而耗尽这个循环中结点的能量。防御 DOS 攻击的方法不固定，它随着攻击者攻击方法的不同而不同。一些跳频和扩频技术可以用来减轻网络堵塞问题，恰当的认证可以防止网络中被插入无用信息。然而，这些协议必须十分有效，否则它也会被用来当作 DOS 攻击的手段。比如，使用基于非对称密码机制的数字签名可以用来进行信息认证，但是创建和验证签名是一个计算速度慢、能量消耗大的计算，攻击者在网络中引入大量的这种信息，就会有效地实施 DOS 攻击。

5.4 结点与组件安全

5.4.1 物联网和传感网的特点

无线传感器网络可以看成由数据获取网络、数据分布网络和控制管理中心三部分组成的。其主要组成部分是集成有传感器、数据处理单元和通信模块的结点，各结点通过协议组成一个分布式网络，再将采集来的数据进行优化，然后经无线电波传输给信息处理中心。

因为结点的数量巨大，而且还处在随时变化的环境中，这就使它有着不同于普通传感器网络的独特“个性”。首先是无中心和自组网特性。在无线传感器网络中，所有结点的地位都是平等的，没有预先指定的中心。各结点通过分布式算法来相互协调，在无人值守的情况下，结点就能自动组织起一个测量网络。而正因为没有中心，网络便不会因为单个结点的脱离而受到损害。

其次是网络拓扑的动态变化性。网络中的结点是处于不断变化的环境中，它的状态也在相应地发生变化，加之无线通信信道不稳定，网络拓扑也在不断地调整变化，而这种变化方式是无法准确预测出来的。

再次是传输能力的有限性。无线传感器网络通过无线电波进行数据传输，虽然省去了布线的烦恼，但是相对于有线网络，低带宽则成为它的天生缺陷。同时，信号之间还存在相互干扰，信号自身也在不断地衰减，不过因为单个结点传输的数据量并不算大，这个缺点还是能忍受的。

最后是能量的限制。为了测量真实世界的具体值，各个结点会密集地分布于待测区域内，人工补充能量的方法已经不再适用。每个结点都要储备可供长期使用的能量，或者自己从外汲取能量（如太阳能）。

5.4.2 WSN 网络结点安全

WSN 网络结点本身的安全性至关重要，传感器结点是构成无线传感器网络的基本单元，如果入侵者能够轻易找到并毁坏各个结点，那么网络的安全性就十分脆弱。无线传感器结点数量众多，少数结点被破坏不会对网络造成太大影响，但是需要保证一些关键结点的安全，如簇首、中心结点、广播结点、认证中心等。这些结点在网络中数量较少但至关重要，一旦被破坏网络将面临完全失效的危险。如果攻击者能够较容易地对上述结点进行物理上的分析和修改，就可利用被俘获的结点干扰网络的正常功能，甚至可能通过分析其内部敏感信息和上层协议机制达到俘获整个网络的目的，这将带来严重的后果。

针对 WSN 结点的攻击方式有很多种。捕获结点攻击时，结点中可能存在冗余密钥，这些密钥信息以一定的概率被其他结点使用，它们被捕获后通过获取其他结点内部的敏感信息作为其他攻击活动的起点。复制结点攻击时，攻击者在捕获结点后得到其密钥信息，利用这些信息来构建恶意结点的密钥。女巫（sybil）攻击时，其中一个恶意结点不断声明有多重身份，使其更易成为路由路径中的结点，然后和其他攻击方法结合使用，达到攻击的目的。拒绝服务（Denial of service，DOS）攻击时，攻击结点以不同的身份连续向某邻居结点发送数据请求报文，使该邻居结点不停地分配资源以维持一个新的连接。芯片是结点的信息处理和控制中心，对结点的攻击往往主要针对芯片发起。对结点芯片的攻击方法可分为以下几类。

逻辑攻击：即通过病毒、后门等对结点的机密性、完整性和可用性造成破坏，或者利用加密算法以及安全协议本身的漏洞进行侵入。WSN 的网络联通性为逻辑攻击的扩散提供了条件。逻辑攻击可能是最危险的袭击，被注射的恶意代码能够传播给网络中的所有结点，潜在地存在毁灭整个网络，而更坏的情况是袭击者控制整个网络。一个被俘的传感器网络可能发送关于环境的错误信息给合法的用户发，或者将监控区域信息发送给恶意的用户。

旁路攻击：指通过观测芯片运行过程中的一些旁路信息如运行时间、功耗、电磁辐射等，推断出隐藏于其中的机密信息。旁路攻击的主要攻击方式包括时间分析攻击、功耗分析攻击、电磁分析攻击以及错误注入攻击，它通常用来破解加密设备的密钥。

侵入式物理攻击：指通过微探测的方式破解芯片的攻击，这是一种破坏性的攻击方法。其主要攻击步骤包括：①打开芯片封装。②实施逆向工程进行版图重建。③使用微探针平台进行探测。其中探针可用于捕获和注入信号，也可用于探测数据总线。

错误注入攻击：通过改变嵌入式设备的外部输入或者环境参数，如工作电压、时钟以及温度等，注入瞬态错误，这种攻击手段可用来：①破坏可用性，如将芯片内部某些总线置为恒定值。②篡改内部程序和数据。③破解密钥。例如当采用中国剩余定理来加速 RSA 算法的私钥签名操作时，对于错误更为敏感，某些错误情况下，错误注入攻击可以求解 RSA 算法的私钥。

5.4.3 密钥管理机制

密钥管理和身份认证在传感器网络中是一个十分具有挑战性的问题。由于传感器结点的资源限制，传统的 PKI 公钥加密体系不适合传感器结点。身份认证在传感器网络中的主要目的是判断结点是否属于同一组织，而不一定需要结点之间互相确认明确的身份，身份认证的工作一般可以与密钥管理结合完成。

传感器网络的密钥管理方案一般可以分为以下几类：①随机密钥预部署。这种方案使用预先分配和加载对称密钥的方法，实现传感器结点之间的保密通信。基于随机密钥的这

类方案简单灵活，在较大范围内得到认可。②中央式的密钥管理方式。这类方案往往需要一个中央机构辅助完成结点之间的密钥维护和密钥管理工作，通常会受到网络规模的限制。③位置敏感密钥管理。这种策略利用位置信息增强传感器网络的安全健壮性，是传感器密钥管理研究的一个新趋势。

5.4.4　网络结点的能耗问题和节能技术

能耗是无线传感器网络所面临的最大问题，因为结点长期处于无人值守的状态，有效的能耗策略必不可少。

目前最常使用的策略是休眠机制，即在结点空闲时使其处于休眠状态，此时其能耗降到最低。但是休眠的结点在转回正常状态的时候往往会消耗大量的能量，因此寻找合理的状态转换策略是确保休眠机制成功的关键。

数据融合是另一项节能技术。多个邻近结点经常会采集同样的信息，发送这些冗余信息就给系统增加了不必要的负担。因此，通过本地计算和筛选，确保发送出最有效的信息就是数据融合的任务。当一个事件发生时，事件周围的传感器结点对该事件有相似的观察结果。通常为了节省宝贵的能量（如果所有结点把它们的观察结果都报告给基站，会导致浪费大量的能量），事件周围的传感器结点会互相合作，通过数据融合的方式产生一份最终报告，并由负责数据融合的结点沿着优化的路径报告给基站，再由基站负责与后台任务处理系统进行通信。

其他能量管理策略还有冲突避免和纠错以及多跳短距离通信等。

5.5　无线传感网安全

5.5.1　无线传感器网络安全问题分析

无线传感器网络的基本任务是准确、及时地提供目标区域的特定事件或者对象的信息，但是其网络的开放性和无线通信的广播特性，使得无线传感器网络存在安全隐患。无线传感器网络的安全问题是一个活跃的研究领域，从无线传感器网络协议的角度来说，WSN 的安全问题可以在四个不同的协议层考虑。

物理层：物理层定义无线接口和用于传输和接收消息的实际方法，如频率、数据率、信号调制方式等。物理层的安全主要取决于安全编码的具体实现方法。在物理层攻击的手段包括拥塞攻击，可采用宽频（跳频）、优先级消息、低占空比、区域映像、模式转换的方法进行防御；物理破坏，可采用破坏证明、结点伪装和隐藏的方法进行防御。

媒体访问控制层：媒体访问控制层定义数据编码和解码的方式、错误发现和修正方式、寻址方案等。媒体访问控制层的安全主要考虑数据帧的加密和认证、访问控制等问题。MAC层的攻击包括碰撞攻击，可采用纠错码技术进行防御；耗尽攻击，可采用设置竞争门限进行防御；针对非公平竞争策略，可采用短帧策略和非优先级策略进行防御。

网络层：网络层基于系统定义的能量和延迟参数建立消息从一个结点到另一个结点的安全可靠的路由。攻击包括洪泛攻击，其防御机制包括客户端谜题；失步攻击，可采用认证方法进行抵御；针对丢弃和贪婪破坏，可使用冗余路径、探测机制进行防御；针对汇聚结点攻击可采用加密和逐跳认证机制进行防御；针对方向误导攻击可采用出口过滤、认证、监视机制进行防御；针对黑洞攻击可采用认证、监视、冗余机制进行防御。

应用层：应用层负责数据管理，最重要的任务是确保数据的正确性，应用层的安全主要关注密钥的管理和交换。

5.5.2 无线传感网安全要求

无线传感网要求传感器存储、处理和传递的信息不被在未授权的情况下获取，具有保密性（Confidentiality）；要求参与信息处理的各个结点的身份真实可信，具有真实性（Authenticity）；要求传输的信息没有受到未授权的篡改或破坏，具有完整性（Integrity）；要求网络中各结点能正常发挥功能，数据能正常提供，具有可用性（Avanability）；要求接收的数据是最新的，而不是攻击者重放的旧信息，具有数据鲜活性（Data Freshness）。

由于低成本、一次性和无人看管的特点，传感器容易被毁坏，易被攻击者物理获取、拆解，直至完全控制。因此，要求无线传感网具有可扩展性（Scalable）和容错性（False Tolerant），在某个或某些结点不能正常工作、增加新结点或对结点进行调整的情况下仍能正常运转。同时要求无线传感网维护由大量易出错、易被控制的传感器组成的传感网，并具有自组织性（Self Organization），能自动组网。

5.5.3 无线传感网安全问题

无线传感网自身的特性给信息安全提出了新的挑战。由于无线传感网的一次性、无人看管、无线通信、低成本、资源受限等特点，传感器容易出现异常。攻击者发动物理攻击、密钥破解、拒绝服务攻击、偷听、流量分析等相对容易。而无线传感网传感器量大和资源受限性也使得设计密钥存储、分发和加解密机制成为一个具有挑战性的问题。

（1）密钥安全问题

大多数安全协议需要采用密码技术并用到密钥，如加密和解密、身份鉴别、签名等。与传统的密钥通过加密方式存储不一样，传感器由于无人看管的原因，需要直接存储自身的密钥信息和密码算法。攻击者通过控制传感器结点，能够获取密钥，从而作为一个内部

合法结点发动一系列攻击。

密码系统中的密钥分为两种类型。一种是对称密钥，加密和解密采用相同的密钥；另一种是非对称密钥，加密和解密采用不同的密钥，并且由加密密钥不能获取解密密钥，反之亦然。由于非对称密钥系统对存储和处理能力要求较高，资源受限的传感器难以胜任，所以在传感器网络中采用较广的是对称密钥。

无线传感网通信方式可以分为三种。一种是两个传感器结点直接通信；第二种是多个传感器组成一个组，组中的某个结点可以向组内成员进行广播消息；第三种是网络中某个结点可以向全网进行广播。根据这三种不同的通信用途，把密钥分为一对结点间密钥、组密钥、广播密钥。在使用对称密钥机制中，一方面由于传感器量大和存储能力有限，在一个传感器中存储该传感器与其他所有传感器通信的密钥，常常是不现实的，这就对密钥的存储机制提出了挑战；另一方面，由于无线传感网存储能力、处理能力和通信能力有限，传统的对称密钥机制也因其复杂性并不能直接应用到无线传感网中。

（2）物理安全问题

1）传感器攻击（Node Compromise）。

与传统的计算机终端有专人保护不一样，传感器部署后，由于无人看管，很难阻止攻击者获取传感器并进行拆解，从而将获得的传感器存储的密码和感知数据用于进一步的攻击。无线传感网安全的一个挑战就是如何限制这些被劫持传感器（Node capture）影响的范围和程度，减小这些被劫持的传感器造成的威胁。

2）传感器异常（Node Malfunction，Node Outage）。

传感器通常部署在恶意环境中，拥有受限的资源，这些传感器会因电源不足等原因停止工作或出现功能异常，给无线传感网的安全带来威胁。

3）覆盖孔洞问题（Coverage Hole）。

一些应用为了容错、冗余或对目标对象精确定位需要在目标区域部署大量传感器，对目标区域进行高度覆盖。但在随机部署过程中或传感器受到攻击时，该区域正常工作的传感器会变稀疏，造成覆盖孔洞，使其不能正常应用。

4）结点复制攻击（The Node Replication Attack）。

在结点复制攻击中，攻击者有意在网络中多个位置放置被控制结点的副本以引起网络的不一致，以达到攻击的目的。

5）无线电干扰（Jamming）。

无线传感器网络中，传感器之间、传感器与基站之间都是通过无线方式进行通信的。攻击者可以在无线传感网区域内发射无线电干扰信号进行干扰，使得无线传感器网络不能正常工作，直至瘫痪。

（3）网络安全问题

无线传感器网络中，恶意的传感器结点可以通过大量占用某个（或某些）传感器的通信资源，使得这个（或这些）传感器的通信资源分配不公正，与其他传感器通信的资源非常少，不能满足正常通信的需要，甚至直接使得这个（或这些）传感器不能与其他传感器进行通信，从而破坏无线传感网的正常运转。

恶意传感器占用其他传感器通信资源的一种方式是恶意传感器结点不停地向某个传感器发送通信请求，造成该传感器的通信资源耗尽。

恶意传感器占用其他传感器通信资源的另一种方式是利用网络通信协议的特点，耗尽被攻击的传感器结点资源。两个无线传感器结点通信时，接收结点通常要验证发送结点传递的信息是否出错，如果出错则要求发送结点重传。一个恶意结点可以在传输的消息中引进一个字节的冲突，不停地向接收结点发送这种含有冲突的信息，导致接收结点因检测到错误而不停地要求重传，从而耗尽接收结点的带宽和能量，达到对接收结点进行攻击的目的。

1）多重身份攻击（Sybil）。

在无线传感网中，恶意的传感器结点可以向其他传感器结点提供多重身份。这样，无线传感网采用的分布式存储、分散性、多路经路由、拓扑结构维护等容错方案的效果就会大大降低，因为这些技术通常期望由多个结点来共同分担风险，却因恶意传感器结点用一个结点冒充了多个结点而达不到共同分担风险的目的。另外，在多重身份攻击已发现的信息传输路径中包含攻击者的可能性大大增加，为后续攻击奠定基础。

2）欺骗、改变、重放路由信息（Spoofed-AlteredReplayed Routing Information）。

路由信息用于建立起一条从源结点向目标结点传递信息的路经。攻击者采用欺骗、改变或重放路由信息的方式可以建立环形的路径让信息永不停息地传递；可以延长或缩短路径长度；可以增加源结点到目标结点的延迟；可以改变网络流量的分布，吸引或分散网络流量；还可以创建错误信息，改变网络结构等。

3）选择转发（Selective Forwarding）。

当源结点建立起向目标结点传通信息的路径后，路径上的恶意结点可以拒绝转发任何数据包，聪明的恶意结点甚至可以有选择地转发某些数据包，包括只转发攻击者自己的信息或沿错误的路径转发等，从而导致传感器结点间不能正常地进行通信。

4）急行军攻击（The Rushing Attack）。

大多数按需路由协议依赖广播 route-request 来发现信息传输路径。在急行军攻击中，攻击者以比合法者更快的速度转发 route-request，从而使在路由协议发现的信息传输路径中包含攻击者的可能性大大增加，为后续攻击奠定基础。

5）虫洞攻击（Wormhole）与核心结点孔洞攻击（Sinkhole）。

在虫洞攻击中，攻击者在网络中一个恶意结点处接收到数据包，然后与网络中另外一个恶意结点建立直接通道，并把数据包直接发给该结点，而跳过在正常传递信息方法中需

要经过的其他结点。由于虫洞攻击中两个恶意结点间传递信息比正常结点传输信息快，它们容易成为各自区域的核心结点。网络中其他传感器愿意聚集在这两个恶意结点周围，选择这两个恶意结点传递信息，给无线传感网造成危害。

虫洞攻击的另外一个特例就是如果恶意结点能直接与基站进行通信，那么该恶意结点周围的其他结点都愿意通过该恶意结点传递信息，这样，该恶意结点就成了该区域的核心结点，从而造成了核心结点孔洞攻击。

6）呼叫洪攻击（Hello Flood）。

很多网络协议要求传感器结点通过广播呼叫数据包（Hello）告知他的邻居们，而接收到该数据包的结点就会认为自己在发送者正常的无线电范围内，发送者是自己的邻居。而一个具有强大发射功率的攻击者可以使无线传感网中每个结点都相信攻击者是自己的邻居。攻击者利用该特性可以开展其他的攻击。

7）确认欺骗攻击（Acknowledgment Spoof）。

很多网络协议中，发送者要求接收者发送确认信息，攻击者可以利用该特性进行确认欺骗攻击。由于无线传感网中传感器结点间通过广播的形式进行通信，攻击者可以监听网络中发给自己邻居的信息，并以那些已经停止工作或不能正常工作的邻居身份发送确认信息，得到确认的发送者就会与这些邻居进行通信，结果当然是失败的，从而达到攻击者的目的。

8）洪拒绝服务攻击（Flood）。

很多网络协议需要保存通信的状态信息，而洪拒绝服务攻击通过大量发送洪信息（如传统的 TCP SYN 包），耗尽结点的存储空间等。

9）同步攻击（Desyn chronization）。

在两个结点进行通信时，通常通过某种机制保持步调一致。而攻击者通过伪造两个结点的一端或两端的信息，破坏这种步调一致性，从而达到攻击的目的。

10）重放攻击（Replay）。

重放攻击中，攻击者发送目标结点已接收过的数据。攻击者既可以通过重放攻击占用目标结点的资源，对目标结点的可用性造成威胁，也可以通过重放身份认证或加密过程的信息绕过安全机制，成为合法用户，对目标结点进行攻击，还可以通过重放旧信息，对数据的鲜活性造成威胁，使得目标结点接收到的是关于事件的过时数据。

11）数据篡改攻击（MeSsage Corruption）和数据注入攻击（Inject Data）。

攻击者通过篡改消息的内容破坏消息的完整性，特别是恶意结点可以向正常消息中注入错误的数据来破坏消息的完整性。

（4）应用安全问题

1）重编程攻击（Reprogram）。

由于传感器结点不能避免被控制，攻击者就可以通过对传感器软件进行重新编程，发

动一系列的攻击。

2）数据融合攻击（Fusion）。

当一个事件发生时，通常事件周围的传感器结点会互相合作，通过数据融合的方式产生一份最终报告，并由负责数据融合的结点报告给基站。然而，如果某些结点被攻击者控制，发送错误的报告，数据融合就会失败。

3）定位服务攻击（Location Services）。

定位信息对于许多基于位置的服务（如目标跟踪）非常关键。而恶意传感器结点通过发布错误的位置信息，造成目标结点定位不准或错误，从而达到攻击的目的。

4）位置隐藏（Source Laation Privacy）。

无线传感网一个重要应用就是监视有价值的目标，而这个目标通常也是攻击者的兴趣所在。因此，隐藏目标的位置信息，防止被攻击者发现至关重要。另外，在无线传感网中，负责数据融合的结点、密钥管理结点、查询监视结点、基站等这些有特殊用途的结点的安全对整个无线传感网安全也至关重要，它们的位置信息也是攻击者的兴趣所在，需要加以隐藏保护。

（5）基站的安全问题

基站是无线传感网连到互联网等外部网络的网关，也是攻击者的重要兴趣目标。如何隐藏基站的位置和身份？如何增加基站的容错能力？这些都是基站要解决的安全问题。同时，传统的联网计算机面临的安全问题也是基站面临的安全问题。

5.6 加密技术

所谓数据加密（Data Encryption）技术是指将一个信息（或称明文，plain text）经过加密钥匙（Encryption key）及加密函数转换，变成无意义的密文（cipher text），而接收方则将此密文经过解密函数、解密钥匙（Decryption key）还原成明文。加密技术是网络安全技术的基石。

这里的加密技术是指对电子信息采取的安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。加密技术的应用是多方面的，但最为广泛的还是在电子商务和 VPN 上的应用，深受广大用户的喜爱。

5.6.1 密钥

（1）密钥的分类

数据加密技术要求只有在指定的用户或网络下，才能解除密码而获得原来的数据，这

就需要给数据发送方和接收方以一些特殊的信息用于加解密，这就是所谓的密钥。其密钥的值是从大量的随机数中选取的。按加密算法分为专用密钥和公开密钥两种。

1）专用密钥。

专用密钥，又称为对称密钥或单密钥，加密和解密时使用同一个密钥，即同一个算法。如 DES 和 MIT 的 Kerberos 算法。单密钥是最简单方式，通信双方必须交换彼此密钥，当需要给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。当一个文本要加密传送时，该文本用密钥加密构成密文，密文在信道上传送，收到密文后用同一个密钥将密文解出来，形成普通文体供阅读。在对称密钥中，密钥的管理极为重要，一旦密钥丢失，密文将无密可保。这种方式在与多方通信时因为需要保存很多密钥而变得很复杂，而且密钥本身的安全就是一个问题。

对称密钥是最古老的，一般说“密电码”采用的就是对称密钥。由于对称密钥运算量小、速度快、安全强度高，目前仍广泛被采用。

DES 是一种数据分组的加密算法，它将数据分成长度为 64 位的数据块，其中 8 位用作奇偶校验，剩余的 56 位作为密码的长度。第一步将原文进行置换，得到 64 位的杂乱无章的数据组；第二步将其分成均等两段；第三步用加密函数进行变换，并在给定的密钥参数条件下，进行多次迭代从而得到加密密文。

2）公开密钥。

公开密钥，又称非对称密钥，加密和解密时使用不同的密钥，即不同的算法。虽然两者之间存在一定的关系，但不可能轻易地从一个推导出另一个。一把公用的加密密钥可能与对应多把解密密钥，如 RSA 算法。

非对称密钥由于两个密钥（加密密钥和解密密钥）各不相同，因而可以在将一个密钥公开，将另一个密钥保密的情况下，同样起到加密的作用。

在这种编码过程中，一个密码用来加密消息，而另一个密码用来解密消息。在两个密钥中有一种关系，通常是数学关系。公钥和私钥都是一组十分长的、数字上相关的素数（是另一个大数字的因数）。有一个密钥不足以翻译出消息，因为用一个密钥加密的消息只能用另一个密钥才能解密。每个用户可以得到唯一的一对密钥，一个是公开的，另一个是保密的。公共密钥保存在公共区域，可在用户中传递，甚至可印在报纸上面。而私钥必须存放在安全保密的地方。任何人都可以有你的公钥，但是只有你一个人能有你的私钥。它的工作过程是：“你要我听你的吗？除非你用我的公钥加密该消息，我就可以听你的，因为我知道没有别人在偷听。只有我的私钥（其他人没有）才能解密该消息，所以我知道没有人能读到这个消息。我不必担心大家都有我的公钥，因为它不能用来解密该消息。”

公开密钥的加密机制虽提供了良好的保密性，但难以鉴别发送者，即任何得到公开密钥的人都可以生成和发送报文。数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、

冒充和篡改等问题。

数字签名一般采用非对称加密技术（如 RSA），通过对整个明文进行某种变换，得到一个值，作为核实签名。接收者使用发送者的公开密钥对签名进行解密运算，如其结果为明文，则签名有效，证明对方的身份是真实的。当然，签名也可以采用多种方式，例如将签名附在明文之后。数字签名普遍用于银行、电子贸易等。

数字签名不同于手写签字。数字签名随文本的变化而变化，手写签字则反映某个人个性特征，是不变的；数字签名与文本信息是不可分割的，而手写签字是附加在文本之后的，与文本信息是分离的。

值得注意的是，能否切实有效地发挥加密机制的作用，关键的问题在于密钥的管理，包括密钥的生存、分发、安装、保管、使用以及作废全过程。

（2）主要功能

1）PKI。

PKI（Public Key Infrastructure）是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务，并提供所必需的密钥和证书管理体系。

原有的单密钥加密技术采用特定加密密钥加密数据，而解密时用于解密的密钥与加密密钥相同，这称之为对称型加密算法。采用此加密技术作为理论基础的加密方法如果用于网络传输数据加密，则不可避免地出现安全漏洞。因为在发送加密数据的同时，也需要将密钥通过网络传输通知接收者，第三方在截获加密数据的同时，只需再截取相应密钥即可将数据解密使用或进行非法篡改。

区别于原有的单密钥加密技术，PKI 采用非对称的加密算法，即将原文加密成密文的密钥不同于将密文解密为原文的密钥，以避免第三方获取密钥后将密文解密。

2）证书。

证书实际是由证书签证机关（CA）签发的对用户公钥的认证。

证书的内容包括：电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期，等等。目前，证书的格式和验证方法普遍遵循 X.509 国际标准。

加密：将文字转换成不能直接阅读的形式（即密文）的过程称为加密。

解密：将密文转换成能够直接阅读的文字（即明文）的过程称为解密。

如何在电子文档上实现签名的目的呢？我们可以使用数字签名。RSA 公钥体制可实现对数字信息的数字签名，方法如下：

信息发送者用其私钥对从所传报文中提取出的特征数据（或称数字指纹）进行 RSA 算法操作，以保证发信人无法抵赖曾发过该信息（即不可抵赖性），同时也确保信息报文在传递过程中未被篡改（即完整性）。当信息接收者收到报文后，就可以用发送者的公钥对数字签名进行验证。

在数字签名中有重要作用的数字指纹是通过一类特殊的散列函数（HASH 函数）生成的。对这些 HASH 函数的特殊要求是：①接收的输入报文数据没有长度限制。②对任何输入报文数据生成固定长度的摘要（数字指纹）输出。③从报文能方便地算出摘要。④难以对指定的摘要生成一个报文，而由该报文可以算出其指定的摘要。⑤难以生成两个具有相同摘要的不同报文。

收方在收到信息后用如下的步骤验证您的签名：①使用自己的私钥将信息转为明文。②使用发信方的公钥从数字签名部分得到原摘要。③收方对您所发送的源信息进行 HASH 运算，也产生一个摘要。④收方比较两个摘要，如果两者相同，则可以证明信息签名者的身份。

如果两摘要内容不符，会说明什么原因呢？

可能对摘要进行签名所用的私钥不是签名者的私钥，这就表明信息的签名者不可信。也可能收到的信息根本就不是签名者发送的信息，信息在传输过程中已经遭到破坏或篡改。

3）数字证书。

数字证书为实现双方安全通信提供了电子认证。在因特网、公司内部网或外部网中，使用数字证书实现身份识别和电子信息加密。数字证书中含有密钥对（公钥和私钥）所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证。

使用数字证书能做什么?

数字证书在用户公钥后附加了用户信息及 CA 的签名。公钥是密钥对应的一部分，另一部分是私钥。公钥公之于众，谁都可以使用，私钥只有自己知道。由公钥加密的信息只能由与之相对应的私钥解密。为确保只有特定收件人才能阅读自己的信件，发送者要用收件人的公钥加密信件，收件人便可用自己的私钥解密信件。同样，为证实发件人的身份，发送者要用自己的私钥对信件进行签名，收件人可使用发送者的公钥对签名进行验证，以确认发送者的身份。

在线交易中您可使用数字证书验证对方身份。用数字证书加密信息，可以确保只有接收者才能解密、阅读原文，同时保证了信息在传递过程中的保密性和完整性。有了数字证书网络安全才得以实现，电子邮件、在线交易和信用卡购物的安全才能得到保证。

认证、数字证书和 PKI 解决的几个问题?

保密性：只有收件人才能阅读信息。

认证性：确认信息发送者的身份。

完整性：信息在传递过程中不会被篡改。

不可抵赖性：发送者不能否认已发送的信息。

4）证书签发机构 CA。

CA 是证书的签发机构，它是 PKI 的核心。CA 是负责签发证书、认证证书、管理已颁

发证书的机关。它要制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权。

CA 也拥有一个证书（内含公钥）和私钥。网上的公众用户通过验证 CA 的签字从而信任 CA，任何人都可以得到 CA 的证书（含公钥），用来验证它所签发的证书。

如果用户想得到一份属于自己的证书，他应先向 CA 提出申请，在 CA 判明申请者的身份后，便为他分配一个公钥，并且在 CA 将该公钥与申请者的身份信息绑在一起，并为之签字后，便形成证书发给申请者。

如果一个用户想鉴别另一个证书的真伪，他就用 CA 的公钥对那个证书上的签字进行验证，一旦验证通过，该证书就被认为是有效的。

5.6.2 数据加密的实现

一般的数据加密可以在通信的三个层次来实现，即链路加密、结点加密和端到端加密。

（1）链路加密

对于在两个网络结点间的某一次通信链路，链路加密能为网上传输的数据提供安全保证。对于链路加密（又称在线加密），所有消息在被传输之前进行加密，在每一个结点对接收到的消息进行解密，然后先使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过许多通信链路的传输。

由于在每一个中间传输结点消息均被解密后重新进行加密，因此包括路由信息在内的链路上的所有数据均以密文形式出现。这样，链路加密就掩盖了被传输消息的源点与终点。填充技术的使用以及填充字符在不需要传输数据的情况下就可以进行加密，这使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

尽管链路加密在计算机网络环境中使用得相当普遍，但它并非没有问题。链路加密通常用在点对点的同步或异步线路上，它要求先对在链路两端的加密设备进行同步，然后使用一种链模式对链路上传输的数据进行加密。这就给网络的性能和可管理性带来了负作用。

在线路/信号经常不通的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。另外，即使仅一小部分数据需要进行加密，也会使得所有传输数据被加密。

在一个网络结点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有结点在物理上必须是安全的，否则就会泄露明文内容。然而保证每一个结点的安全性需要较高的费用，为每一个结点提供加密硬件设备和一个安全的物理环境所需要的费用由以下几部分组成：保护结点物理安全的雇员开销，为确保安全策略和程序的正确执行而进行审计时的费用，以及为防止由于安全性被破坏产生的损失而参加保险的费用。

在传统的加密算法中，用于解密消息的密钥与用于加密的密钥是相同的，该密钥必须

被秘密保存，并按一定规则进行变化。这样，密钥分配在链路加密系统中就成了一个问题，因为每一个结点必须存储与其相连接的所有链路的加密密钥，这就需要对密钥进行物理传送或者建立专用网络设施。而网络结点地理分布的广阔性使得这一过程变得复杂，同时增加了密钥连续分配时的费用。

（2）结点加密

尽管结点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的：两者均在通信链路上为传输的消息提供安全性保障；都在中间结点先对消息进行解密，然后进行加密；因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。

然而，与链路加密不同，结点加密不允许消息在网络结点以明文形式存在。它先把收到的消息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在结点上的一个安全模块中进行。

结点加密要求报头和路由信息以明文形式传输，以便中间结点能得到如何处理消息的信息。因此这种方法在防止攻击者分析通信业务方面是脆弱的。

（3）端到端加密

端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密（又称脱线加密或包加密），消息被传输时在到达终点之前不进行解密，因为消息在整个传输过程中均受到保护，所以即使有结点被损坏也不会使消息泄露。

端到端加密系统的价格便宜些，并且与链路加密和结点加密相比更可靠，更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此外，从用户对安全需求的直觉上讲，端到端加密更自然些。单个用户可能会选用这种加密方法，以便不影响网络上的其他用户，此方法只需要源和目的结点是保密的即可。

端到端加密系统通常不允许对消息的目的地址进行加密，这是因为每一个消息所经过的结点都要用此地址来确定如何传输消息。由于这种加密方法不能掩盖被传输消息的源点与终点，因此它在防止攻击者分析通信业务方面是脆弱的。

5.6.3　加密技术的应用

加密技术的应用是多方面的，但最为广泛的还是在电子商务和 VPN 上的应用，下面就分别简叙。

（1）在电子商务方面的应用

电子商务（E-business）要求顾客可以在网上进行各种商务活动，不必担心自己的信用卡会被人盗用。在过去，用户为了防止信用卡的号码被窃取，一般是通过电话订货，然后使用用户的信用卡进行付款。现在人们开始用 RSA（一种公开/私有密钥）的加密技术，提

高信用卡交易的安全性，从而使电子商务走向实用成为可能。

许多人都知道 NETSCAPE 公司是 Internet 商业中领先技术的提供者，该公司提供了一种基于 RSA 和保密密钥的技术应用于因特网，该技术被称为安全插座层（Secure Sockets Layer，SSL）。

也许很多人知道 Socket，它是一个编程界面，并不提供任何安全措施，而 SSL 不但提供编程界面，而且向上提供一种安全的服务。SSL3.0 现在已经应用到了服务器和浏览器上，SSL2.0 则只能应用于服务器端。

SSL3.0 用一种电子证书（electric certificate）来实行身份验证后，双方就可以用保密密钥进行安全的会话了。它同时使用“对称”和“非对称”加密方法。在客户与电子商务的服务器进行沟通的过程中，客户会产生一个 Session Key，然后客户用服务器端的公钥将 Session Key 进行加密，再传给服务器端。在双方都知道 Session Key 后，传输的数据都是以 Session Key 进行加密与解密的，但服务器端发给用户的公钥必须先向有关发证机关申请，以得到公证。

基于 SSL3.0 提供的安全保障，用户就可以自由订购商品并且给出信用卡号了，也可以在网上和合作伙伴交流商业信息并且让供应商把订单和收货单从网上发过来，这样可以节省大量的纸张，为公司节省大量的电话、传真费用。在过去，电子信息交换（Electric Data Interchange，EDI）、信息交易（information transaction）和金融交易（financial transaction）都是在专用网络上完成的，使用专用网的费用大大高于互联网。正是这样巨大的诱惑，才使人们开始发展因特网上的电子商务，但不要忘记数据加密。

（2）加密技术在 VPN 中的应用

现在，越多越多的公司走向国际化，一个公司可能在多个国家都有办事机构或销售中心，每一个机构都有自己的局域网 LAN（Local Area Network）。但在当今的网络社会中人们的要求不仅如此，用户还希望将这些 LAN 连接在一起组成一个公司的广域网，这个在现在已不是什么难事了。

事实上，很多公司都已经这样做了，但它们一般租用专用线路来连结这些局域网，它们考虑的就是网络的安全问题。现在具有加密/解密功能的路由器已普及，这就使人们通过互联网连接这些局域网成为可能，这就是我们通常所说的虚拟专用网（Virtual Private Network，VPN）。当数据离开发送者所在的局域网时，该数据首先被用户端连接到互联网上的路由器进行硬件加密，数据在互联网上是以加密的形式传送的，当达到目的 LAN 的路由器时，该路由器就会对数据进行解密，这样目的 LAN 中的用户就可以看到真正的信息了。

第 6 章　无线传感网的设计与测评

6.1　WSN 协议框架设计

在无线传感器网络的各层中存在着许多协议，它是定义通过网络进行通信的规则，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息，以这种规则规定双方完成信息在计算机之间的传送过程。下面就对网络协议规范作个框架概述，其中大部分还是沿用的有线网络的协议。

ARP（Address Resolution Protocol）地址解析协议。它是用于映射计算机的物理地址和临时指定的网络地址。启动时它选择一个协议（网络层）地址，并检查这个地址是否已经有别的计算机使用。如果没有被使用，此结点可以使用这个地址；如果此地址已经被别的计算机使用，正在使用此地址的计算机会通告这一信息，此协议会另选地址。

SNMP（Simple Network Management P）网络管理协议。它是 TCP/IP 协议中的一部分，它为本地和远端的网络设备管理提供了一个标准化途径，是分布式环境中的集中化管理的重要组成部份。

AppleShare protocol（AppleShare 协议）。它是 Apple 机上的通信协议，它允许计算机从服务器上请求服务或者交换文件。AppleShare 可以在 TCP/IP 协议或其他网络协议如 IPX、AppleTalk 上进行工作。使用它时，用户可以访问文件、应用程序、打印机和其他远程服务器上的资源。它可以和配置了 AppleShare 协议的任何服务器进行通信，Macintosh、Mac OS、Windows NT 和 Novell Netware 都支持 AppleShare 协议。

AppleTalk 协议。它是 Macintosh 计算机使用的主要网络协议。Windows NT 服务器有专门针对 Macintosh 的服务，也能支持该协议。其允许 Macintosh 的用户共享存储在 Windows NT 文件夹的 Mac 格式的文件，也可以使用和 Windows NT 连接的打印机。Windows NT 共享文件夹以传统的 Mac 文件夹形式出现在 Mac 用户面前。Mac 文件名按需要被转换为 FAT

（8.3）格式和 NTFS 文件标准。支持 Mac 文件格式的 DOS 和 Windows 客户端能与 Mac 用户共享这些文件。

BGP4（Border Gateway Protocol Vertion 4）边界网关协议−版本 4。它是用于自治网络中网关主机（每个主机有自己的路由）之间路由信息的协议，它使管理员能够在已知的路由策略上配置路由加权，可以更方便地使用无级内部域名路由（CIDR），它是一种在网络中可以容纳更多地址的机制，它比外部网关协议（EGP）更新。BGP4 经常用于网关主机之间，主机中的路由表包括了已知路由的列表、可达的地址和路由加权，这样就可以在路由中选择最好的通路。BGP 在局域网中通信时使用内部 BGP（IBGP），因为 IBGP 不能很好工作。

BOOTP 协议。它是一个基于 TCP/IP 协议的协议，它可以让无盘站从一个中心服务器上获得 IP 地址，现在人们通常使用 DHCP 协议进行这一工作。

CMIP（Common Management Information Protocol）通用管理信息协议。它是建立在开放系统互连通信模式上的网络管理协议。相关的通用管理信息服务（CMIS）定义了访问和控制网络对象、设备和从对象设备接收状态信息的方法。

Connection-oriented Protocol/Connectionless Protocol 面向连接的协议/无连接协议。在广域网中，这种协议是两台计算机建立物理连接过程所使用的，这种物理连接要持续到成功地交换完数据为止。在 Internet 中，TCP（传输控制协议）即这一类型的协议，它为两台连接在网络上的计算机提供了可相互通信且确保数据成功传输的一种手段。面向连接的协议一定要保证数据传送到对方。Internet 中的 IP 协议无连接协议，IP 只关注将数据分成数据包进行传输，并在这些数据包被接收后重新组包，而不关注接收方计算机的状态。由面向连接的协议（如 Internet 中的 TCP）来确保数据的接收。

DHCP（Dynamic Host Configuration Protocol）动态主机配置协议。它是在 TCP/IP 网络上使客户机获得配置信息的协议，它是基于 BOOTP 协议，并在 BOOTP 协议的基础上添加了自动分配可用网络地址等功能。这两个协议可以通过一些机制互相操作。DHCP 协议在安装 TCP/IP 协议和使用 TCP/IP 协议进行通信时，必须配置 IP 地址、子网掩码、默认网关三个参数，这三个参数可以手动配置，也可以使用 DHCP 自动配置。

Discard Protocol 抛弃协议。它的作用就是接收到什么抛弃什么，它对调试网络状态有一定的用处。基于 TCP 的抛弃服务，如果服务器实现了抛弃协议，服务器就会在 TCP 端口 9 检测抛弃协议请求，在建立连接并检测到请求后，就直接把接收到的数据抛弃，直到用户中断连接。而基于 UDP 协议的抛弃服务和基于 TCP 差不多，检测的端口是 UDP 端口 9，功能也一样。

Echo Protocol 协议。这个协议主要用于调试和检测中，作用也十分简单，就是将接收到的信息原封发回。它可以基于 TCP 协议，服务器就在 TCP 端口 7 检测有无消息，如果有发

送来的消息就直接返回。如果使用 UDP 协议的基本过程和 TCP 一样，检测的端口也是 7。

FTP（File Transfer Protocol）文件传输协议。它是一个标准协议，是在计算机和网络之间交换文件的最简单的方法。与传送可显示文件的 HTTP 和电子邮件的 SMTP 一样，FTP 也是应用 TCP/IP 协议的应用协议标准。FTP 通常用于将网页从创作者手中上传到服务器上供人使用，而从服务器上下传文件也是一种非常普遍的使用方式。作为用户，您可以用非常简单的 DOS 界面来使用 FTP，也可以使用由第三方提供的图形界面的 FTP 来更新（删除，重命名，移动和复制）服务器上的文件。现在有许多服务器支持匿名登录，允许用户使用 FTP 和 ANONYMOUS 作为用户名进行登录，通常可使用任何口令或只按回车键。

HDLC（High-Level Data Link Control）高层数据链路协议。它是一组用于在网络结点间传送数据的协议。在 HDLC 中，数据被组成一个个的单元（称为帧）通过网络发送，并由接收方确认收到。HDLC 协议也管理数据流和数据发送的间隔时间。HDLC 是在数据链路层中最广泛、最实用的协议之一。现在作为 ISO 的标准，HDLC 是基于 IBM 的 SDLC 协议的，SDLC 被广泛用于 IBM 的大型机环境之中。在 HDLC 中，属于 SDLC 的被称为通常响应模式（NRM）。在通常响应模式中，基站（通常是大型机）发送数据给本地或远程的二级站。不同类型的 HDLC 被用于使用 X.25 协议的网络和帧中继网络，这种协议可以在局域网或广域网中使用，无论此网是公共的还是私人的。

HTTP1.1（Hypertext Transfer Protocol Vertion 1.1）超文本传输协议−版本 1.1。它是用来在 Internet 上传送超文本的传送协议。它是运行在 TCP/IP 协议族之上的 HTTP 应用协议，它可以使浏览器更加高效，使网络传输减少。任何服务器除了包括 HTML 文件以外，还有一个 HTTP 驻留程序，用于响应用用户请求。您的浏览器是 HTTP 客户，向服务器发送请求，当浏览器中输入了一个开始文件或点击了一个超级链接时，浏览器就向服务器发送了 HTTP 请求，此请求被送往由 IP 地址指定的 URL。驻留程序接收到请求，在进行必要的操作后回送所要求的文件。

HTTPS（Secure Hypertext Transfer Protocol）安全超文本传输协议。它是由 Netscape 开发并内置于其浏览器中，用于对数据进行压缩和解压操作，并返回网络上传送回的结果。HTTPS 实际上应用了 Netscape 的完全套接字层（SSL）作为 HTTP 应用层的子层。HTTPS 使用端口 443，而不是像 HTTP 那样使用端口 80 来和 TCP/IP 进行通信。SSL 使用 40 位关键字作为 RC4 流加密算法，这对于商业信息的加密是合适的。HTTPS 和 SSL 支持使用 X.509 数字认证，如果需要的话用户可以确认发送者是谁。

ICMP（Internet Control Message Protocol）Internet 控制信息协议。ICMP 协议是一种面向连接的协议，用于传输出错报告控制信息。它是一个非常重要的协议，对于网络安全具有极其重要的意义。它是 TCP/IP 协议族的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据

无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。ICMP 提供一致易懂的出错报告信息。发送的出错报文返回到发送原数据的设备，因为只有发送设备才是出错报文的逻辑接收者。发送设备随后可根据 ICMP 报文确定发生错误的类型，并确定如何才能更好地重发失败的数据包。但是 ICMP 唯一的功能是报告问题而不是纠正错误，纠正错误的任务由发送方完成。我们在网络中经常会使用到 ICMP 协议，比如我们经常使用的用于检查网络通不通的 Ping 命令（Linux 和 Windows 中均有），这个“Ping”的过程实际上就是 ICMP 协议工作的过程。还有其他的网络命令如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。

IMAP4（Internet Mail Access Protocol Version 4）Internet 邮件访问协议−版本 4。它是用于从本地服务器上访问电子邮件的标准协议，它是一个 C/S 模型协议，用户的电子邮件由服务器负责接收保存。IMAP4 改进了 POP3 的不足，用户可以通过浏览信件头来决定是不是要下载此信件，还可以在服务器上创建或更改文件夹或邮箱，删除信件或检索信件的特定部分。在用户访问电子邮件时，IMAP4 需要持续访问服务器。在 POP3 中，信件是保存在服务器上的，当用户阅读信件时，所有内容都会被立刻下载到用户的机器上。我们有时可以把 IMAP4 看成一个远程文件服务器，把 POP3 可以看成一个存储转发服务。

NNTP（Network News Transfer Protocol）网络新闻传输协议。NNTP 同 POP3 协议一样，也存在某些局限性。

IOTP（Internet Open Trading Protocol）Internet 开放贸易协议。Internet 开放贸易协议是一系列的标准，它使电子购买交易在客户、销售商和其他相关部分都是一致的，无论使用何种付款系统。强调该协议与付费系统是独立的，可接入各种安全支付系统。IOTP 适用于很多的付款系统，如 SET、DigiCash、电子支票或借记卡。付款系统中的数据封装在 IOTP 报文中。IOTP 处理的交易可以包括客户、销售商、信用支票、证明、银行等部分。IOTP 使用 XML 语言（Extensible Markup Language）来定义包含在交易中的数据。在现实世界中，在购买一件商品时，你可能考虑许多因素，如向谁购买，是亲自购买还是通过电话，付款方式，送货方式等。在虚拟世界中，IOTP 保证所有这些都已成功且安全地完成。

IOTP 主要用于以下几个方面。

1）消费者：消费者对销售商和付款的选择范围更大。一致的交易接口节省时间，减少混乱。对每个交易都有记录，方便了消费者和纳税。

2）销售商：销售商可以提供很多现有的和将要有的付款系统。通过标准的数据，销售商可以获取更多的消费者支持，跟踪纳税所需数据。IOTP 使新销售商更容易地加入 Internet 市场。

3）付款系统提供商：因为 IOTP 封装了付款系统的数据，新的付款系统将更易更换。

4）银行：使用 IOTP 银行可以更有效地从销售商那里收取费用，同时银行的业务机会

将增加，因为 IOTP 使新销售商更容易地加入到电子商务中。对 IOTP 的发展做出贡献的有：惠普、IBM、JCP、Master Card International、Smart Card Integrations、Sun Microsystems 和 Wells Fargo 银行。

IPX/SPX（Internetwork Packet Exchange/Sequential Packet Exchange）互联网包交换/顺序包交换。它是由 Novell 提出的用于客户/服务器相连的网络协议。使用 IPX/SPX 协议能运行需要 NetBEUI 支持的程序，通过 IPX/SPX 协议可以跨过路由器访问其他网络。Internet 分组交换/顺序分组交换 IPX/SPX（Internetwork Packet Exchange/Sequences Packet Exchange）是 Novell 公司的通信协议集。与 NetBEUI 形成鲜明区别的是 IPX/SPX 比较庞大，在复杂环境下具有很强的适应性。这是因为 IPX/SPX 在设计一开始就考虑了网络的问题，因此它具有强大的路由功能，适合大型网络使用。当用户端接入 NetWare 服务器时，IPX/SPX 及其兼容协议是最好的选择。但在非 Novell 网络环境中，一般不使用 IPX/SPX。

IPX 主要实现网络设备之间连接的建立维持和终止；SPX 协议是 IPX 的辅助协议，主要实现发出信息的分组、跟踪分组传输，保证信息完整无缺的传输。

IPX/SPX 协议即 IPX/SPX 协议的组合。它是 Novell 公司为了适应网络的发展而开发的通信协议，具有很强的适应性，安装方便，同时还具有路由功能，可以实现多网段间的通信。其中，IPX 协议负责数据包的传送，SPX 负责数据包传输的完整性。在微软的 NT 操作系统中，一般使用 NWLink IPX/SPX 兼容协议和 NWLink NetBIOX 两种 IPX/SPX 的兼容协议，即 NWLink 协议，该兼容协议继承了 IPX/SPX 协议的优点，更适应 Windows 的网络环境。IPX/SPX 协议一般可以应用于大型网络（比如 Novell）和局域网游戏环境中（比如反恐精英、星际争霸）。不过，如果不是在 Novell 网络环境中，一般不使用 IPX/SPX 协议，而是使用 IPX/SPX 兼容协议，尤其是在 Windows 9x/2000 组成的对等网中。通常要在“高级 TCP/IP 设置\WINS”启用 TCP/IP 上的 NetBIOS，以加强局域网的兼容性。IPX 协议全称为 Internetwork Packet Exchange（网间数据包交换），IPX 协议是 Novell NetWare 自带的最底层网络协议，主要用来控制局域网内或局域网之间数据包的寻址和路由，只负责数据包在局域网中的传送，并不保证消息的完整性，也不提供纠错服务。

在局域网中传输数据包时，如果接收结点在同一网段内，通过 IPX 协议就直接按该结点的 ID 将数据传给它；如果接收结点不在同一网段内，那么通过 IPX 协议可以将数据包交给 NetWare 服务器，再继续传输。在使用过程中，网络管理员可以通过使用相应的 IPX 路由命令，比如“routing ipx add/set staticroute”表示在 IPX 路由表中添加或配置静态 IPX 路由，“routing ipx set global”表示配置全局 IPX 路由设置。SPX 协议全称为 Sequences Packet Exchange（顺序包交换），SPX 协议是基于施乐的 Xerox SPP（Sequences Packet Protocol，顺序包协议）协议，同样是由 Novell 公司开发的一种用于局域网的网络协议。在局域网中，SPX 协议主要负责对整个传输的数据进行无差错处理，即纠错。SPX 协议一般和上面介绍的 IPX 协议组合成 IPX/SPX 协议来使用，多用于 Netware 网络环境以及联网游戏。

MIME（Multi-Purpose Internet Mail Extensions）多功能 Internet 邮件扩展。MIME 是扩展 SMTP 协议，是 1991 年 Nathan Borenstein 向 IETF 提出的。在传输字符数据的同时，允许用户传送另外的文件类型，如声音、图像和应用程序，并将其压缩在 MIME 附件中。因此，新的文件类型也被作为新的被支持的 IP 文件类型。

NetBEUI（NetBIOS Enhanced UserInterface）网络基本输入/输出系统扩展用户接口。NetBEUI 协议是 IBM 于 1985 年提出的。NetBEUI 主要为 20～200 个工作站的小型局域网设计的，用于 NetBEUI、LanMan 网、Windows For Workgroups 及 Windows NT 网。NetBEUI 是一个紧凑、快速的协议，但由于 NetBEUI 没有路由能力，即不能从一个局域网经路由器到另一个局域网，已不能适应较大的网络。如果需要路由到其他局域网，则必须安装 TCP/IP 或 IPX/SPX 协议。

OSPF（Open Shortest Path First）开放最短路优先。OSPF 是用于大型自主网络中替代路由信息协议的协议标准。像 RIP 一样，OSPF 也是由 IETF 设计用做内部网关协议族中的一个标准。在使用 OSPF 时网络拓朴结构的变化可以立即在路由器上反映出来。不像 RIP，OSPF 不是全部当前结点保存的路由表，而是通过最短路优先算法计算得到的最短路，这样可以降低网络通信量。如果熟悉最短路优先算法就会知道，它是一种只涉及网络拓朴结构的算法而不涉及其他情况，如优先权的问题。对于这一点，OSPF 改变了算法使它根据不同的情况给某些通路以优先权。

POP3（Post Office Protocol Version 3）邮局协议−版本 3。它是一个关于接收电子邮件的客户/服务器协议。电子邮件由服务器接收并保存，在一定时间之后，由客户电子邮件接收程序检查邮箱并下载邮件。POP3 内置于 IE 和 Netscape 浏览器中。另一个替代协议是交互邮件访问协议（IMAP）。使用 IMAP 可以将服务器上的邮件视为本地客户机上的邮件。在本地机上删除的邮件还可以从服务器上找到。E-mail 可以被保存在服务器上，并且可以从服务器上找回。

PPP（Point to Point Protocol）点对点协议。它是用于串行接口的两台计算机通信协议，是通过电话线连接计算机和服务器而彼此通信而制定的协议。网络服务提供商可以提供点对点连接，这样提供商的服务器就可以响应用户请求，将用户请求接收并发送到网络上，然后将网络上的响应送回。PPP 是使用 IP 协议，有时它被认为 TCP/IP 协议族的一员。PPP 协议可用于不同介质上包括双绞线、光纤和卫星传输的全双工协议，它使用 HDLC 进行包的装入。PPP 协议既可以处理同步通信也可以处理异步通信，可以允许多个用户共享一个线路，又可进行 SLIP 协议所没有的差错控制。

RIP（Routing Infomation Protocol）路由信息协议。RIP 是最早的路由协议之一，而且现在仍然在广泛使用。它从类别上应该属于内部网关协议（IGP）类，它是距离向量路由式协议，这种协议在计算两个地方的距离时只计算经过的路由器数目，如果到相同目标有两

个不等速或带宽不同的路由器，但是经过的路由器的个数一样，RIP 认为两者距离一样，而实际传送数据时，很明显一个快一个慢，这就是 RIP 协议的不足之处，而 OSPF 在它的基础上克服了 RIP 的缺点。

SLIP（Serial Line Internet Protocol）串行线路 Internet 协议。它是一个 TCP/IP 协议，它用于在两台计算机之间通信。通常计算机与服务器连接的线路是串行线路，而不是多路线路或并行线。服务器提供商可以向用户提供 SLIP 连接，这样服务器就可以响应用户请求，并将请求发送到网络上，然后将网络返回的结果送至用户计算机。目前已逐渐被功能更好的 PPP 点对点协议所取代。

SMB protocol（Server Message Block protocol）服务器信息块协议。它提供了运行在客户计算机上的程序请求网络上服务器服务的方法，它可以用于 TCP/IP 协议之上，也可以用于网络协议如 IPX 和 NetBEUI 之上。使用 SMB 协议时，应用程序可以访问远程计算机上的资源，包括打印机、命名管道等。因此，用户程序可以读、创建和更新远程服务器上的文件，也可以和已经安装 SMB 协议的计算机通信。Microsoft Windows for Workgroups、Windows 95 和 Windows NT 都提供了 SMB 协议客户和服务器的支持。对于 UNIX 系统，共享软件 Samba 也提供了类似的服务。

LMTP（Local Mail Transfer Protocol）本地邮件传输协议。SMTP 和 SMTP 服务扩展（ESMTP）提供了一种高效安全传送电子邮件的方法，而在实现 SMTP 时需要管理一个邮件传送队列，在有些时候这样做可能有麻烦，需要一种没有队列的邮件传送系统，而 LMTP 就是这样的一个系统，它使用 ESMTP 的语法，而它和 ESMTP 可不是一回事，而 LMTP 也不能用于 TCP 端口 25。LMTP 协议与 SMTP 和 ESMTP 协议很像，为了避免和 SMTP 和 ESMTP 服务混淆，LMTP 使用 LHLO 命令开始一个 LMTP 会话，它的基本语法和 HELO 和 EHLO 命令相同。对于 DATA 命令来说，如果 RCPT 命令失败，DATA 命令必须返回 503，并失败。每个 DATA 命令碰到“.”时，服务器必须对所有成功的 RCPT 命令返回应答，这和平常的 SMTP 系统不同，而且顺序必须和 RCPT 成功的顺序一致，即使对于同一个向前路径来说有许多 RCPT 命令，也必须返回多个成功应答。这就意味着，服务器返回的确认应答是指服务器把邮件发送到接收者或另一个转发代理。

SMTP（Simple Mail Transfer Protocol）简单邮件传送协议。它是用来发送电子邮件的 TCP/IP 协议。它的内容由 IETF 的 RFC 821 定义。另外一个和 SMTP 相同功能的协议是 X.400。SMTP 的一个重要特点是它能够在传送中接力传送邮件，传送服务提供了进程间通信环境（IPCE），此环境可以包括一个网络、几个网络或一个网络的子网。传送系统（或 IPCE）不是一对一的是很重要的。进程可能直接和其他进程通过已知的 IPCE 通信。邮件是一个应用程序或进程间通信。邮件可以通过连接在不同 IPCE 上的进程跨网络进行邮件传送。更特别的是，邮件可以通过不同网络上的主机接力式传送。

TCP/IP 协议起源于美国国防高级研究计划局。提供可靠数据传输的协议称为传输控制协议 TCP，好比货物装箱单，保证数据在传输过程中不会丢失；提供无连接数据包服务的协议称为网络协议 IP，好比收发货人的地址和姓名，保证数据到达指定的地点。TCP/IP 协议是互联网上广泛使用的一种协议，使用 TCP/IP 协议的 Internet 等网络提供的主要服务有：电子邮件、文件传送、远程登录、网络文件系统、电视会议系统和万维网。它是 Internet 的基础，它提供了在广域网内的路由功能，而且使 Internet 上的不同主机可以互联。从概念上，它可以映射到四层：网络接口层，这一层负责在线路上传输帧并从线路上接收帧；Internet 层，这一层中包括了 IP 协议，IP 协议生成 Internet 数据包，进行必要的路由算法，IP 协议实际上可以分为四个部分：ARP、ICMP、IGMP 和 IP；再上向就是传输层，这一层负责管理计算机间的会话，这一层包括两个协议 TCP 和 UDP，由应用程序的要求不同可以使用不同的协议进行通信；最后一层是应用层，就是我们熟悉的 FTP、DNS、TELNET 等。熟悉 TCP/IP 是熟悉 Internet 的必由之路。

TELNET Protocol 虚拟终端协议。目的是提供一个相对通用的，双向的，面向八位字节的通信方法，它主要的目标是允许接口终端设备的标准方法和面向终端的相互作用。是让用户在远程计算机登录，并使用远程计算机上对外开放的所有资源。

Time Protocol 时间协议。该协议提供了一个独立于站点的，机器可读的日期和时间信息。时间服务返回的是秒数，是从 1900 年 1 月 1 日午夜到现在的秒数。设计这个协议的一个重要目的在于，网络上的许多主机并没有时间的观念，在分布式的系统上，我们可以想一想，北京的时间和东京的时间如何分呢？主机的时间往往可以人为改变，而且因为机器时钟内的误差而变得不一致，因此需要使用时间服务器通过选举方式得到网络时间，让服务器有一个准确的时间观念。不要小看时间，这对于一些以时间为标准的分布运行的程序简直是太重要了。这个协议可以工作在 TCP 和 UDP 协议下。时间是由 32 位表示的，是自 1900 年 1 月 1 日 0 时到当前的秒数，我们可以计算一下，这个协议只能表示到 2036 年就不能用了，但是我们也知道计算机发展速度这么快，到时候可能就会有更好的协议代替这个协议。

TFTP（Trivial File Transfer Protocol）小文件传输协议，它是一个网络应用程序，它比 FTP 简单，也比 FTP 功能少。它在不需要用户权限或目录可见的情况下使用，它使用 UDP 协议而不是 TCP 协议。TFTP 是一个传输文件的简单协议，它基于 UDP 协议而实现，但是我们也不能确定有些 TFTP 协议是基于其他传输协议完成的。此协议设计的时候是进行小文件传输的。因此它不具备通常的 FTP 的许多功能，它只能从文件服务器上获得或写入文件，而不能列出目录，不能进行认证，它传输 8 位数据。传输中有三种模式：netascii，这是 8 位的 ASCII 码形式；另一种是 octet，这是 8 位源数据类型；最后一种 mail 已经不再支持，它将返回的数据直接返回给用户而不是保存为文件。任何传输起自一个读取或写入文件的请求，这个请求也是连接请求。如果服务器批准此请求，则服务器打开连接，数据以

定长 512 字节传输。每个数据包包括一块数据，服务器发出下一个数据包以前必须得到客户对上一个数据包的确认。如果一个数据包小于 512 字节，则表示传输结束。如果数据包在传输过程中丢失，发出方会在超时后重新传输最后一个未被确认的数据包。通信的双方都是数据的发出者与接收者，一方传输数据接收应答，另一方发出应答接收数据。大部分的错误会导致连接中断，错误由一个错误的数据包引起。这个包不会被确认，也不会被重新发送，因此另一方无法接收到。如果错误包丢失，则使用超时机制。错误主要由下面的情况引起的：不能满足请求，收到的数据包内容错误，而这种错误不能由延时或重发解释，对需要资源的访问丢失（如硬盘满）；TFTP 只在一种情况下不中断连接，这种情况是源端口不正确，在这种情况下，指示错误的包会被发送到源机。这个协议限制很多，这些都是为了实现起来比较方便而进行的。因为 TFTP 使用 UDP，而 UDP 使用 IP，IP 还可以使用其他本地通信方法。因此一个 TFTP 包中会有以下几段：本地媒介头、IP 头、数据包头、TFTP 头，剩下的就是 TFTP 数据了。TFTP 在 IP 头中不指定任何数据，但是它使用 UDP 中的源和目标端口以及包长度域。由 TFTP 使用的包标记（TID）在这里被用做端口，因此 TID 必须介于 0～65535 之间。

UDP（User Datagram Protocol）用户数据包协议，它是定义用来在互连网络环境中提供包交换的计算机通信协议，此协议默认网路协议（IP）是其下层协议。UDP 是 TCP 的另外一种方法，像 TCP 一样，UDP 使用 IP 协议来获得数据单元（叫做数据包），不像 TCP，它不提供包（数据包）的分组和组装服务。而且，它还不提供对包的排序，这意味着，程序必须自己确定信息是否完全正确地到达目的地。如果网络程序要加快处理速度，那么 UPD 就比 TCP 要好。UDP 是 OSI 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。UDP 协议基本上是 IP 协议与上层协议的接口。UDP 协议适用端口分别运行在同一台设备上的多个应用程序。UDP 协议的全称是用户数据包协议，在网络中它与 TCP 协议一样用于处理 UDP 数据包，是一种无连接的协议。在 OSI 模型中，第四层——传输层，处于 IP 协议的上一层。UDP 有不提供数据包分组、组装和不能对数据包进行排序的缺点，也就是说，当报文发送之后，是无法得知其是否安全完整到达的。UDP 用来支持那些需要在计算机之间传输数据的网络应用。包括网络视频会议系统在内的众多客户/服务器模式的网络应用都需要使用 UDP 协议。UDP 协议从问世至今已经被使用了很多年，虽然其最初的光彩已经被一些类似协议所掩盖，但是即使在今天 UDP 仍然不失为一项非常实用和可行的网络传输层协议。与所熟知的 TCP（传输控制协议）协议一样，UDP 协议直接位于 IP（网际协议）协议的顶层。根据 OSI（开放系统互连）参考模型，UDP 和 TCP 都属于传输层协议。

UDP 协议的主要作用是将网络数据流量压缩成数据包的形式。一个典型的数据包就是一个二进制数据的传输单位。每一个数据包的前 8 个字节用来包含报头信息，剩余字节则

用来包含具体的传输数据。在选择使用协议的时候，选择 UDP 必须要谨慎。在网络质量令人不十分满意的环境下，UDP 协议数据包丢失会比较严重。但是由于 UDP 的特性：它不属于连接型协议，因而具有资源消耗小、处理速度快的优点，所以通常音频、视频和普通数据在传送时使用 UDP 较多，因为它们即使偶尔丢失一两个数据包，也不会对接收结果产生太大影响。比如我们聊天用的 ICQ 和 QQ 就是使用的 UDP 协议。UDP 报头由 4 个域组成，其中每个域各占用两个字节，具体如下：

UDP 源端口号、目标端口号、数据包长度、校验。UDP 协议使用端口号为不同的应用保留其各自的数据传输通道。UDP 和 TCP 协议正是采用这一机制来实现对同一时刻内多项应用同时发送和接收数据的支持。数据发送一方（可以是客户端或服务器端）将 UDP 数据包通过源端口发送出去，而数据接收一方则通过目标端口接收数据。有的网络应用只能使用预先为其预留或注册的静态端口；而另外一些网络应用则可以使用未被注册的动态端口。因为 UDP 报头使用两个字节存放端口号，所以端口号的有效范围是 0～65535。一般来说，大于 49151 的端口号都代表动态端口。数据包的长度是指包括报头和数据部分在内的总字节数。因为报头的长度是固定的，所以该域主要被用来计算可变长度的数据部分（又称为数据负载）。数据包的最大长度根据操作环境的不同而各异。从理论上说，包含报头在内的数据包的最大长度为 65535 字节。不过，一些实际应用往往会限制数据包的大小，有时会降低到 8192 字节。UDP 协议使用报头中的校验值来保证数据的安全。校验值首先在数据发送方通过特殊的算法计算得出，在传递到接收方之后，还需要再重新计算。如果某个数据包在传输过程中被第三方篡改或者由于线路噪声等原因受到损坏，发送和接收方的校验计算值将不会相符，由此 UDP 协议可以检测是否出错。这与 TCP 协议是不同的，后者要求必须具有校验值。许多链路层协议都提供错误检查，包括流行的以太网协议，为什么 UDP 也要提供检查和校验。其原因是链路层以下的协议在源端和终端之间的某些通道可能不提供错误检测。虽然 UDP 提供有错误检测，但检测到错误时，UDP 不做错误校正，只是简单地把损坏的消息段扔掉，或者给应用程序提供警告信息。

6.2 WSN 路由设计

6.2.1 WSN 路由协议的特点

我们要针对无线传感器网络设计新的路由协议，必须清楚地了解其网络层的特点，知道为什么不能使用传统 Ad hoc 中的路由协议。

从宏观上看，无线传感器网络的数据传输遵循多对一（Many To One）的模式，这是一种收敛播（Convergecast）。Sink 结点是无线传感器网络中的特殊结点，起着非常关键的作

用，经常作为网关与 Internet 相连接，它远离感知区域，向传感器结点发送控制命令，传感器结点在感知或接收到新数据后，经过中间结点的转发和融合，最终的目的是要将数据传送到 Sink 结点，由 Sink 结点进行分析、加工，转换成人们所需的信息。从宏观上看，这是传统网络很少用到的一种通信模式——收敛播，图 6-1 所示为这种通信模式。

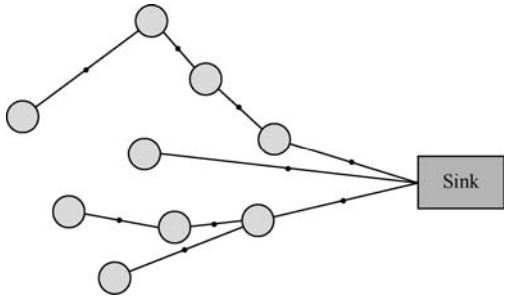


图 6-1　收敛播

无线传感器网络是以数据为中心（Data Centric）进行路由的。不同于传统 Ad Hoc 网络以地址为中心（Address Centric）进行路由的模式，以数据为中心进行路由是无线传感器网络网络层的一个显著特点。与之相反，我们把传统网络称为以地址为中心或以结点为中心进行路由。在无线传感器网络中人们只关心某个区域的某个观测指标的值，而不会去关心具体某个结点的观测数据，比如说人们可能希望知道“检测区域的东北角上的温度是多少”，而不会关心“地址为 8 的结点所探测到的温度值是多少”，这就是传感器网络的以数据为中心的特点。而传统网络传送的数据是和结点的 IP 地址联系起来的，以数据为中心的特点要求传感器网络能够脱离传统网络的寻址过程，快速有效地组织起各个结点的信息并融合提取出有用信息直接传送给用户。

图 6-2 说明了以数据为中心进行路由和以地址为中心进行路由的区别。

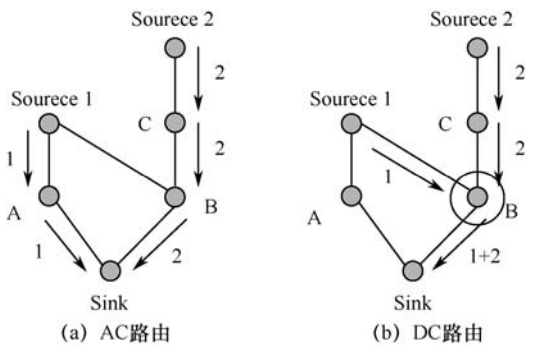


图 6-2　以数据为中心进行路由和以地址为中心进行路由

无线传感器网络邻近结点间采集的数据具有相似性，存在冗余信息，需经数据融合（Data Fusion）处理再进行路由；由于传感器最基本任务就是感知、采集数据，在无线传感器网络中，数量庞大的无线传感器密集分布在感知区域，地理位置邻近的结点间采集的数据必然具有相似性，如果不对这些相似的数据进行数据融合，将会产生大量冗余信息。直接将这些未经处理、存在冗余的数据进行传输，将会造成网络带宽、结点能源的巨大浪费，导致结点迅速死亡，缩短整个网路的生命周期。

无线传感器网络的结点易于失效，且数量远远大于传统的 Ad Hoc 网络中的结点数，而结点的处理能力、存储能力和通信能力却远低于传统 Ad Hoc 网络中的结点；无线传感器网络中传感器结点分布密集，数量巨大，可能达到几万、几十万，甚至更多，而对于每个无线传感器结点来说，其处理能力、存储能力和通信能力无法和传统 Ad Hoc 网络中的结点——便携式计算机相提并论。如何在这种结点数量巨大，单个结点易于失效且资源极其有限的网络中进行路由就成了前所未有的挑战。

无线传感器网络中的大部分结点不像传统 Ad hoc 网络中的结点一样快速移动，因此没有必要花费很大的代价频繁地更新路由表信息。在传统 Ad hoc 网络中，由于应用的要求，结点频繁移动，动态变化的拓扑结构是传统 Ad hoc 网络最显著的特点，快速有效地达到路由协议收敛状态是其路由协议的首要目标。而对于无线传感器网络，除了原有结点失效和新的结点加入外，拓扑结构基本不会发生变化，因此没有必要花费很大的代价频繁地更新路由表信息。

单向信道的存在会对路由协议带来影响。常规路由协议通常认为底层的通信信道是双向的。但是在采用无线通信的无线传感器网络环境中，由于发射功率或地理位置等因素的影响，可能存在单向信道。它为常规路由协议带来三个严重的影响：认知单向性、路由单向性和汇点不可达。

由于无线传感器网络层以上特点，使得传统网络的路由协议如 RIP、OSPF 以及传统的 Ad Hoc 网络路由协议如 AODV（Ad hoc demand distancevector）和 TORA（Temporally Order Routing Algorithm）都不适用于无线传感器网络，无线传感器网络需要设计新的路由协议。

6.2.2 无线传感器网络路由协议的要求

传统计算机网络对路由协议要求如下：正确性、健壮性、稳定性、公平性、最优性。无线传感器网络对路由协议也有以上要求，但它更注重以下特殊要求。

能源有效性：由于无线传感器网络结点能量有限，所以路由协议设计必须将有效利用能源放在第一位，将服务质量（QoS）放在第二位考虑。能量有限性是传感器结点最显著的特点，无线传感器结点体积小、价格低廉，大多采用电池作为能源提供者，要想在几年内将目前的电池的可供电时间提高 30%都是很困难的。典型的无线传感器网络工作在人类

无法忍受的恶劣的环境中，甚至是人类无法到达环境，比如火山周围。一旦电池耗尽，将无法更换，设计有效的路由协议节约结点能源、延长网络的生命周期就成为无线传感器网络的核心问题。为无线传感器网络设计的路由协议应提供节能策略，比如设备“睡眠”机制，而且，进入“睡眠”状态的结点不能对路由协议的正常运行产生负作用。

简单性：相对于传统网络而言，传感器结点的运算能力和存储能力极其有限，这种硬件资源有限的结点却承担着主机和路由器的双重角色，这就要求我们不能照搬传统网络路由协议的设计思想，要为这种结点资源有限的特殊网络“量身定制”一种简单有效的路由协议，要求路由协议的报文和算法简单有效，实现的程序代码短小精悍，路由表项尽可能少。

多路性：典型的无线传感器网络工作在人类无法忍受的恶劣的环境中，各种情况经常会使得结点失效，为了避免单个结点的失效影响整个网络的效率，要求每个结点尽可能维护多条路由。维护多条路由是指每个结点同时维护去往 Sink 结点的多条路由，只有当所有路由都失效时，才按需发起路由请求过程，从而降低了路由请求频率、分组等待延时和协议开销。

6.2.3　无线传感器网络路由协议的分类

无线传感器网络路由协议的分类基本上延续了传统 Ad hoc 网的分类方法，不同的角度可以进行不同的分类。根据路由发现策略的角度，可分为主动路由和被动路由两种类型；根据网络管理的逻辑结构可将路由协议分为平面路由和分层结构路由两类。

主动路由：也叫表驱动（Table Driven）路由，主动路由的路由发现策略与传统路由协议类似，结点通过周期性地广播路由信息分组，交换路由信息，主动发现路由，同时，结点必须维护去往全网所有结点的路由。它的优点是当结点需要发送数据分组时，只要去往目的结点的路由存在，所需的延时很小。缺点是主动路由需要花费较大的开销，应尽可能使得路由更新能够紧随当前拓扑结构的变化。而且，动态变化的拓扑结构可能使得这些路由更新变成过时信息，路由协议始终处于不收敛状态。传统的路由协议如 RIP，OSPF 都属于主动路由协议。主动路由协议一般包括“邻居结点探测”和“路由广播”两个过程。路由器向各通信端口周期广播 Hello 分组，来实现邻居结点探测。在距离矢量算法中，虽然没有显式的邻结点探测过程，但在与邻结点交换距离向量路由表时，隐含了邻结点探测。

被动路由：也叫按需（On Demand）路由，与主动路由相反，被动路由认为在动态变化的网络环境中，没有必要维护去往其他所有结点的路由。它仅在没有去往目的结点路由的时候才“按需”进行路由发现。被动路由协议根据网络分组的传输请求，被动地搜索从源结点到目的结点的路由。当没有分组传递请求时，路由器处于静默状态，并不需要交换路由信息。拓扑结构和路由表内容按需建立，它可能仅仅是整个拓扑结构信息的一部分。

它的优点是不需要周期性的路由信息广播，节省了一定的网络资源。缺点是发送数据分组时，如果没有去往目的结点的路由，数据分组需要等待因路由发现引起的延时。

被动路由协议主要包括“路由发现”和“路由维护”两个过程。当源结点需要获得到目的结点的路由，而该路由又没有在路由表中时，路由发现过程被激活。路由器采用泛洪的方式，向整个网络广播路由请求分组。当有路由请求报文到达目的结点时，目的结点将向源结点发出路由请求应答报文。这样，在源与目的结点之间会建立起双向“活动路径”。活动路径建立所需时间定义为路由建立延迟。随着拓扑结构的变化，当活动路径上的某段链路发生中断时，路由维护过程被启动。路由维护可以采用两种不同的策略：从断点处开始修补路径或通知源结点重新启动路由建立过程。

被动路由协议是自组网特有的路由协议类型，它可以降低路由消耗，提高网络的吞吐量。但是，被动路由协议具有潜在的不确定性，包括目标结点是否可达的不确定性和路由建立延迟不确定。

平面路由：平面结构是指网络中各结点在路由功能上地位相同，没有引入分层管理机制。平面结构路由的优点是网络中没有特殊的结点，网络流量均匀地分散在网络中，路由算法易于实现。缺点是可扩展性小，在一定程度上限制了网络的规模。

分层路由：与平面路由协议相对应的是分层结构的路由协议。分层路由协议采用簇的概念对传感器结点进行层次划分。若干个相邻结点构成一个簇，每一个簇有一个簇首。簇与簇之间可以通过网关通信。网关可以是簇首也可以是其他簇成员。网关之间的连接构成上层骨干网，所有簇间通信都通过骨干网转发。

分层路由协议包括成簇协议、簇维护协议、簇内路由协议和簇间路由协议四个部分。成簇协议解决如何在动态分布式网络环境下使移动结点高效地聚集成簇，它是分层路由协议的关键。簇维护协议要解决在结点移动过程中的簇结构维护，其中包括移动结点退出和加入簇，簇的产生和消亡等功能。分层路由协议比较适合无线传感器网络，但成簇过程会产生一定的能源消耗，如何产生有效的簇类也正是各地学者深入研究的问题。

无线传感器网络的路由协议目前正是国外研究的热点，各种路由协议在不同的应用环境和性能评价指标下各有千秋。

6.3 WSN 协议测评

随着无线传感器网络研究的不断深入，应用化已经逐渐成为人们关注的焦点。各种在特定应用背景下的研究层出不穷，如环境监测、目标跟踪、安全监控等。与传统的网络相比，无线传感器网络所包含的结点数量巨大，应用环境复杂多变，如何对这些应用研究成

果进行验证和测试，以保证其在实际工作中稳定高效，已经成为亟待解决的问题。

目前大多数研究都通过理论分析和计算机模拟的方法进行验证和测试。理论分析的方法虽然可以进行多个同类协议的比较，但数学模型的构建由于计算复杂度过高，在应用这些模型解决实际问题时需要做大量简化，从而降低了理论性能分析的可信度。现有的模拟工具则由于难以真实体现无线通信的不稳定性，其验证的效果也无法令人满意。而通过传感器结点建立网络测试平台，可以在实际应用过程中验证测试网络的协议和算法，不仅比较全面地包含了影响网络状态的各个因素，而且也避免了因模型简化导致的理论误差。因此无线传感器网络的平台测试技术越来越被人们所关注。

由于无线传感器网络应用环境的不确定性、网络系统的动态性以及无线通信的不可靠性，使得在搭建无线传感器网络测试平台时，面临着三个关键问题：①如何准确地对结点及网络的各种状态信息并进行量化评估，即如何进行网络测试；②如何实时地获得结点及网络状态值，并在此基础上调整和改变结点运行参数以及网络行为，即如何进行网络监控；③如何使由实际结点组成的网络测试平台能够反映大规模网络部署以及实际应用环境的特征，即如何搭建测试平台。本节将分别从上述三个方面对无线传感器网络平台测试的关键技术进行详细的介绍和讨论。

（1）网络测试

无线传感器网络的状态可以分为结点状态和网络状态两部分。点状态主要包括结点的剩余能量、缓冲区使用情况以及结点间链路质量等本地状态；而网络状态则包括网络能量分布、链路质量分布以及网络拓扑分布等，是对结点状态的一个全局性的归纳和描述。

目前国内外无线传感器网络测试评估技术还没有形成标准化和系统化，研究主要针对无线传感器网络无线通信不稳定和资源能量有限的两大特点，测试其网络链路质量（吞吐率、延迟、丢包率等）和结点剩余能量、网络生存时间。下面我们就这两方面内容分别进行介绍。

1）无线链路测试。

无线通信容易受到天气和空间环境等外界因素的干扰，变化复杂且不稳定，不容易量化和评估。目前虽然很多通信协议的开发者都会对无线传感器网络的链路质量进行测试，但测试的方法和内容往往针对自身的协议和特定的应用背景，不具有一般性。

美国加州大学（UCLA）提出一种专门用于无线传感器网络链路质量测试的工具 SCALE。SCALE 系统建立在 EmStar 平台上，由多个运行 TinyOS 系统的 Mote 结点和一台便携式计算机组成。各个结点通过串口与计算机相连，使得结点的数据分组一方面可以由无线通信装置进行收发，一方面可以由串口传输给计算机，从而通过比较两个结果对网络数据分组转发的情况进行分析并研究其概率统计规律。SCALE 系统轻便易携，可以方便地应用于各种环境中。

在 SCALE 中，结点周期的发送包含结点 ID、序列号的探测分组数据包，研究人员通过观测这些探测数据分组转发的概率统计规律，研究链路通信的特性，如不同条件下分组转发速率与通信距离的关系，分组转发速率与链路非对称性的关系，分组转发速率与分组大小的关系以及链非对称性与通信距离的关系等，从而对协议算法的研究进行验证和指导。

分组探测方法虽然可以有效地衡量通信链路的质量，但对链路上其他数据的干扰较大。实验表明，在当结点数据发送速率达到每秒两个分组时，分组测量方法可能无法正常工作。研究人员在此基础上，进一步提出了一种通过机器学习技术对链路质量进行预测评估的方法，即针对如何测试网络整体的通信性能进行研究，并给出了高效性、公平性、平衡性以及延时等评估标准。

2）能量消耗测试。

测试无线传感器网络结点及网络的能量消耗一直是一个困难的问题。由于结点的能量状态值始终在动态变化，而且结点对其能量状态进行测试的过程本身也消耗能量，因此理论上结点的能量状态是无法准确测试的。在 Power TOSSIM、AEON 等能量测试技术中，预先测量结点在不同工作状态下的功耗，然后结点在实际工作过程中统计自身处于各个状态的时间，从而得出结点总共消耗的能量。这种方法对于统计无线通信模块、传感器模块等慢速模块比较适用，但 CPU 处于忙碌状态的时间往往很短，结点很难准确统计自身 CPU 的工作时间。

上述测试方法主要针对单个结点的能量消耗。但当网络规模较大时，很难实现对每个结点持续地进行能量扫描和状态收集。因此，Ber kley 的研究人员提出了针对网络整体能量消耗的测试技术 eScan。eScan 利用 GPS 等方法对结点进行精确定位，利用 APM（高级电源管理）和 ACPI（高级配置和能量接口）方法对结点剩余能量进行测量。结点在剩余能量大幅下降时提交报告，通过发散和汇集算法，将位置相邻且能量相近的结点合并为一个区域。这样只需向服务器发送各个区域的能量和位置信息就可以描述整个网络的剩余能量状况，得到能量等高分布图，如图 6-3 所示。这种方法在保证收集信息精度的情况下，大大减少了能量信息收集过程中的通信量，从而降低了扫描过程的能量损耗。

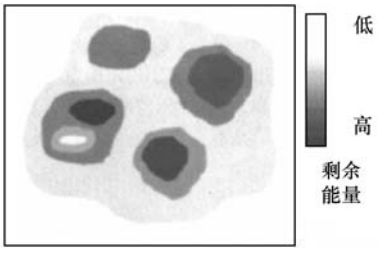


图 6-3　eScan 能量等高分布图

eScan 虽然能够整体性地描述网络能量的使用和分布状况，但其对每个结点精确定位的要求，对于资源有限的无线传感器网络来说难以实现。另外，在 eScan 中所采用的能量测试方法（APM 和 ACPI）是否适用于无线传感器网络，也缺乏实际应用的验证。事实上，对能量测试的评估算法进行验证也是十分困难的：一方面，通过理论模型的验证方法存在着固有的计算误差；另一方面，如果通过实验，等待结点出现能量耗尽，往往需要几周甚至更长的时间，也不太现实。

基于上述情况，德国柏林大学的研究人员提出了一种在小规模无线传感器网络中，对网络能量消耗的实验性测量方法。他们将网络和结点生存时间量化为能够完成工作周期的最大次数，然后利用 GoldCaps 大容量电容为每个传感器结点进行供电。使用这种电容，可以保证结点在每十秒钟发送一个数据包的发送速率下持续工作 70 多分钟。这样便可以在较短的时间内实际测得网络每个结点完成工作周期的最大次数。获得实际测量值后，通过与相同条件下理论分析的结果进行比较，一方面验证了上述理论分析的准确性；另一方面可以得到理论值与实际值的误差比，从而对理论分析值进行修正。

利用 GoldCaps 电容可以在实际网络应用过程中进行能量测试，从而避免了因为理论模型简化而造成的测量误差。但是利用工作周期数来量化结点的能量消耗，本身也只能是对能量的一种近似估计。

（2）网络监控

由于无线传感网络部署环境复杂多变，用户预先设定的结点和网络工作方式难以保证长期适用。因此在实际工作过程中越来越需要及时了解网络状态的变化并进行网络行为的调整，即需要对无线传感网络进行监控。网络平台测试对网络的监控化要求则更为明显：一方面需要准确实时地获取结点及网络的各种状态信息及其变化，从而对网络中运行的各种协议和算法性能进行测试评估；另一方面需要不断地改变网络行为甚至结点系统结构，模拟不同应用环境中的网络运行状况，以配合测试的需要。

1）网络监视。

目前国外无线传感器网络监控工具主要针对于特定的传感器结点以及特殊的应用背景，功能比较局限，适应性和可扩展性不强。比如国际著名公司 Crossbow 针对其系列传感器结点及网络为用户提供了一个网络监控平台 MoteWorks。MoteWorks 平台分为网络、服务器和客户端三层。网络中每个结点上运行 TinyOS 系统和 XMesh 协议栈支持包括 ZigBee 在内的多种网络协议，并通过 XOtap 支持对结点的无线编程和远程更新；在服务器端通过运行 XServer 服务器软件将传感器结点网络与 Internet 网络连接起来；在客户端，用户可以通过运行 MoteView 客户端软件登录 XServer 服务器与传感器结点网络进行交互，图形化地查看各个结点的状态、能量（电压）的使用情况，以及链路传输速率等网络特征，并远程调整传感器结点发送功率半径、传感器感应类型等参数。还有由波士顿大学信息与系统工程中心（CISE）发起的名为 Millennial Net 的项目给各种工业及商业无线传感器网络提供解

决方案的同时，也提供了网络监控的工具，通过图形化的检测界面，使得用户可以设置网络以及设备运行的参数并监视网络各个组件的状态以及 I/O 连接情况。这些已有的工具虽然都实现了一定的监测功能，但都与特定的应用背景紧密相关，而且所监测的网络信息往往与网络实际应用中的数据信息混合显示，并没有形成系统地针对各种应用的监视工具。

2）网络控制。

目前对于无线传感器网络的控制主要通过重编程技术实现，即将用户指令传输到网络结点上以调整结点运行参数甚至系统内容，进而改变网络行为，实现对网络的控制。重编程技术可以按照层次进行划分，目前比较流行的是划分为三个层次：编码层（Programming Layer），指用户向网络发出的用于改变网络行为的指令代码内容；传输层（Transmission Layer），主要为网络结点中传输的数据；执行层（Execution Layer），具体在结点上执行的程序内容。

国内外对重编程的研究技术目前可以分为两种，针对指令执行的/支持（support）技术和针对代码编写的抽象（abstraction）技术。支持技术将编码层和传输层的功能合并，用户指令直接传输到结点上进行执行。此类技术的代表包括通过虚拟机技术实现基于应用组件操作的 Mate 系统；根据 Tcl 脚本语言组合调用结点上各种 API 的 Sensor-Ware 系统；利用中间件的结构对网络应用进行模型化的 Impala 系统。而抽象技术是将传输层与执行层的功能结合，对网络的行为进行抽象，提炼出可读性强的语言指令。这些指令在网络中进行编译传输，最终在结点上执行。其主要代表为对网络局部行为进行抽象的 TinyGlas 系统和对网络全局行为进行抽象的 Kairos 系统。

支持技术所需要传输的数据量小，指令执行效率高，但只能满足网络系统升级的需要，适用功能有限。而抽象技术虽然提供了理解性和扩展性更强的指令形式，但对网络的负担较大。因此现在对重编程技术的研究倾向于将两种技术结合起来。由 TinyOS 系统开发者提出的 Active Sensor Network 框架，在 Mate 的基础上对网络行为进行了抽象，为用户提供了可读性强的指令形式。而指令进入网络后，首先转化 Mate 系统原有的脚本执行语言，再发送至结点进行执行。

（3）测试平台

无线传感器网络不仅结点规模大，网络所应用的地域规模也很大，即使通过实际的传感器结点建立无线传感器网络平台进行测试也无法真实再现相同的应用场景。因此如何能够反映出大规模网络环境，并对各种网络应用具有扩展性，成为平台搭建首先需要考虑的问题。国内外对于测试平台搭建技术的研究还处于初始阶段，现有的一些如 MoteWorks 和 EmStar 等无线传感器网络平台，虽然支持网络测试的功能，但都局限于特定的结点和应用，测试内容也比较单一。目前针对于测试而设计的无线传感器网络平台，比较著名的有 MoteLab 和 Kansei 两种，下面将分别进行介绍。

1）MoteLab 平台。

MoteLab 是哈佛大学开发的一种无线传感器网络测试平台，支持包括 Web 方式在内的

多种用户访问方式，使全世界的用户都可以通过 Internet 对测试平台的网络进行远程操作，从而进行网络测试。MoteLab 的系统结构如图 6-4 所示，由两部分组成：传感器结点网络和中心服务器。

网络中的每个传感器结点为 Mica2 或者 MicaZ 结点，使用 IEEE 802.15.4 协议进行通信；同时这些结点又被连接在 MIB-600 开发板上通过串口与中心服务器相连，并接入以太网。这样使得结点的数据可以通过无线通信装置和串口及以太网等多种渠道进行传输，从而对网络状态进行测试。另外，用户对网络的控制指令也可以通过以太网发送到结点上，在不影响网络应用的情况下对结点实施实时的控制调整。

中心服务器是整个 MoteLab 的主体部分，包含了数据库、管理软件和互联网接口等重要组件，提供了试验任务管理、日程调度、结点重编程、数据日志记录和用户访问管理等功能。数据库通过 MySQL 实现，用于存储管理网络数据；Web 服务器通过 PHP 技术实现，为用户提供了通过 Web 页面访问数据库的方式；数据库日志管理组件（DBLogger）是数据库与结点网络的接口，从网络中收集上来的数据经过它的分类筛选存入数据库；后台任务组件（JobDaemon）用于系统任务的创建与注销，包括对结点进行重编程及数据库的整理等工作。

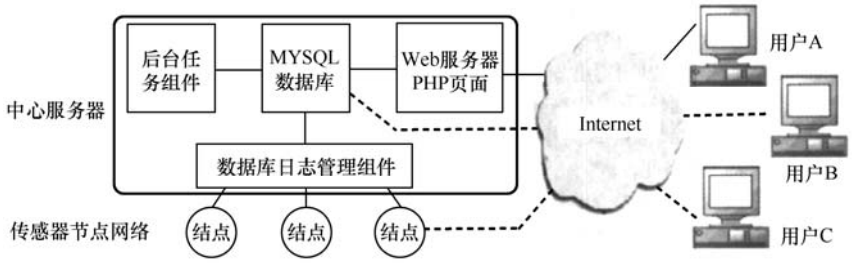


图 6-4　MoteLab 的系统结构

MoteLab 平台为用户提供了 3 种不同的访问途经：①Web 网页访问，用户可以通过 Web 服务器上载任务文件，并启动后台任务组件进行执行，也可以通过 Web 页面对数据库进行查询；②数据库访问，用户通过互联网直接访问后台的数据库，查询下载数据进行分析处理；③网络结点访问，通过 Internet 直接登录到结点进行操作。

MoteLab 这种支持 Web 页面的访问方式实现了开放式的平台资源共享，所提供的多种访问途经使得用户可以更为方便灵活地完成测试任务并对网络进行监控。而且 MoteLab 的开发者认为这种 Web 访问的方式将会成为无线传感器网络平台搭建技术的趋势。但 MoteLab 对于测试评估的方法考虑较少，对能量的测试目前也只是通过在一个结点上连接万用表测电压的方法实现。另外 MoteLab 所支持的网络规模较小，扩展性不强。

2）Kansei 平台。

俄亥俄州立大学开发的 Kansei 平台是面向多种应用的针对无线传感器网络的测试平

台。Kansei 平台在设计上充分考虑了对大规模应用环境的支持及对各种应用背景的通用化和可扩展性的要求，为无线传感器网络测试平台的搭建提供了启发性的思路。

从结构上划分，Kansei 平台由静止网络、便携网络和移动网络 3 部分组成。静止网络是由 210 个结点组成的矩形规则阵列，每个结点分为 XSM 结点和 Stargate 单板计算机两部分。XSM 结点使用 916MHz 微波通信（更新的版本使用了 IEEE 802.15.4 协议通信），是网络测试和控制的对象；Stargate 拥有独立的系统使用 IEEE 802.11b 的协议通信，与以太网相连并可以通过一个 51 脚的连接器对 XSM 进行访问和控制。移动网络由 5 个机器小车组成，行驶于静止网络结点上面铺设的玻璃板上。移动网络结点可以用于收集反馈信号并向静止网络实时注入数据，从而配合静止网络完成测试。便携网络中结点数量不定，除了进行数据存储、压缩、传输和时间同步的管理以外，根据不同试验的需求选择搭配不同的传感器，用于在实际的应用环境中进行数据的感应和采集。

静止网络和移动网络共同构成了 Kansei 系统中的测试通用平台部分，部署在实验室环境中。便携网络则根据测试应用类型选择相应的传感器，部署到实际的测试环境中进行数据采集。便携网络所采集的数据通过以太网发送至 Kansei 的软件平台 Director 上。在 Director 中先对数据建立基于物理参数特性的模型，再通过概率插值等方法将数据扩展到静止网络和移动网络中，从而建立了一个混合模拟的通用测试平台（每个结点都可以模拟扩充为多个结点），以供研究者进行测试。

Kansei 平台的 3 种网络结构为搭建真实反映大规模应用环境的测试平台提供了可行性思路。首先，利用部署、回收便利的便携网络可以在实际的环境条件下进行数据采集，从而更加真实地反映了数据的空间特性和应用特点，而且便携网络的设计也提高了 Kansei 平台面对多种应用的扩展性和灵活性。其次，通过实际结点与理论模拟相结合的混合模拟方法，有效地解决了测试平台网络结点规模不够大的问题。最后，移动网络的设计使得 Kansei 平台可以对移动无线传感器网络应用进行测试评估，网络结构更加丰富灵活。不过目前 Kansei 平台还处于开发过程中，如系统访问控制等功能并没有完全实现，混合模拟方法的效果也有待进一步验证。

6.4 WSN 协议试运行与验收

随着无线通信网络技术的发展和应用，无线通信网络传输技术的应用已不再局限于传统的商业办公领域，而逐步进入到工业制造领域。应用于工业环境中的无线传感器网络的诸多优势包括安装便捷、移位灵活、成本低，能避免工厂环境中“天罗地网”般连线的混乱局面。在工业环境中，对信号传输的实时性和可靠性要求非常高，为了研究无线传感器

网络（Wireless Sensor Network，WSN）的网络延时等因素对实时控制性能的影响，必须提出相应的网络性能测试和分析评价方法。同时，对 WSN 的网络性能进行分析评价，获得网络性能的总体情况，可以评估鉴定和验收一个现有网络。而对于一个待建的网络，如何合适地选择网络结构与部署网络结点，其方案的论证也极大地依赖于对网络性能的分析与评价。目前，针对 WSN 性能的研究主要集中于协议或算法对网络性能的影响上。目前，针对无线传感器网络的性能指标没有统一标准。针对普通 IP 网有一些相关的研究，国际上主要有两大机构针对 IP 网络性能参数指标展开研究。

IETF 的 IP 性能指标工作组提出了定义性能指标的原则与总体框架，并定义了评估 IP 网络数据传输业务的质量、性能和可靠性的一些指标，如连通性、单向时延、环回时延、丢包率、时延变化等。

ITU-T 的第 13 研究组提出了 Y.1540（原 I.380）建议，其中定义了衡量 IP 分组传输性能的 4 个参数：速度（speed）、精确性（accuracy）、可靠性（dependability）和可用性（availability）。并定义了一系列性能指标，如传输时延、时延变化、包错误率、丢包率、虚假 IP 包率、包吞吐量、字节吞吐量等。在进行 WSN 性能评价时，参考以上的性能指标，并遵循指标选取的三大原则（全面性、易测性和相关性）选取合适的指标。在确定了 WSN 的性能指标后，使用线性加权法进行多指标综合评价，其基本步骤为先确定各性能指标的权重，再对决策矩阵作标准化处理，最后求出各待评价目标性能的线性加权平均值。在确定指标权重时，结合主观的权重分析方法（相对比较法）和客观的权重确定方法（变异系数法）进行组合计算，有效地解决了以往单一的客观分析法或单一的主观分析法计算所造成的片面性和局限性，为科学决策提供依据。性能评价将从用户的角度考虑 WSN 的性能，即用户能否接收到某种具有具体性能指标要求（例如时延、抖动、有效带宽、丢包率等）的服务。同时考虑到在对实际或设计的网络本身进行性能评价时，单个的指标有时并不能反映网络的整体性能，因而利用多指标的综合评价，即将多个指标转化为一个能够反映网络综合情况的指标来进行评价，以此来评估和验证传感器网络的整体性能。

集成了传感器、微机电系统和网络三大技术而形成的无线传感器网络是一种全新的信息获取和处理技术，具有十分广阔的应用前景。众所周知，开发、调试和验证无线传感器网络程序是非常困难的。由于无线传感器网络的特殊性，大多数传统 PC 程序的调试手段都不适合无线传感器网络程序。现在调试无线传感器网络程序采用的手段包括串口调试、闪灯（LEDs）调试和模拟器调试。闪灯调试主要借助结点上的闪灯设备的颜色变化来观测程序的执行情况，如可以设定当某个变量的值为零时红灯闪烁。但是结点上面的闪灯数量有限，提供的信息也比较少，无法用它来调试逻辑比较复杂的程序。串口调试则是通过串口程序将结点的状态信息返回 PC 端，它可以很好地观测与 PC 相连的结点内部的执行逻辑，但是对网络中不与 PC 相连接的结点内部执行情况则一无所知，而且结点中的程序如果发

生死锁或崩溃会使得串口以未知的方式失去反应。闪灯调试和串口调试都要求必须实际部署大量的结点，而这需要耗费大量的人力、物力和时间。模拟器调试则是在 PC 上模拟程序的执行，不需要实际部署结点，它可以观测所有结点的内部执行逻辑，而且可以很方便地观察程序的整体行为，具有串口调试和闪灯调试所无可比拟的优势。当然，无线传感器网络的程序相对于传统 PC 程序最大的区别就是程序行为高度依赖于应用环境。在 PC 上模拟调试的程序必须在真实的应用环境下作适应性验证。从无线传感器网络诞生的那一刻起，其仿真模拟器的开发就一直备受重视。国外对于这个领域已经进行了深入的研究，提出了不少理论模型，并且已经开发出了一些实用的仿真模拟器；国内由于进入该领域较晚，现在还没有具体的成果。

（1）典型仿真模拟器分析

TOSSIM 是现在最为流行的无线传感器网络仿真模拟器，它是由美国加州大学伯克利分校的 Philip Levis、Intel 研究中心的 Nelson Lee、哈佛大学的 MattWelsh 等人合作开发的，内嵌在 TinyOS 操作系统中。正如其设计者所宣称的那样，TOSSIM 是一个 TinyOS 程序模拟器，因此它的使用受到了许多限制：

1）只能选用 TinyOS 所支持的 Mica 系列硬件平台。

2）只能使用 NC（一种组件化的 C 语言变种）来编写程序。

3）只有在代码编写完成之后才可以运行模拟器。

换句话说，TOSSIM 其实是一个代码模拟器，只能对整个应用程序进行模拟。如果想模拟协议的话，必须模拟整个程序，只不过将其中的标准协议组件替换为自己的协议组件。当然，TOSSIM 和 TinyOS 的捆绑也有很多优点：TOSSIM 和 TinyOS 命令是集成在一起的，提供了一个统一的界面，使用起来很方便；TOSSIM 可以直接使用 TinyOS 的工具集，如 TinyOS 为 TOSSIM 提供了 GDB 调试功能；TOSSIM 利用了 TinyOS 的组件化结构特点简化了自身的实现机制，所以 TOSSIM 自身的代码规模在所有无线传感器网络仿真模拟器中是最小的。在设计无线传感器网络仿真模拟器时的一个重要考虑就是要在适应大规模结点、高效率和高精度这三者之间取得平衡。TOSSIM 的设计思路非常巧妙，很好地解决了上述问题。

Avrora 是一个程序模拟器，由加州大学洛杉矶分校的 Ben L. Titzer、Jens Palsberg 和康奈尔大学的 Daniel K. Lee 等人开发。Avrora 的设计目标是提供一个 AVR 模拟和分析框架，它不局限于 TinyOS 程序，可以模拟所有基于 AVR 指令集的无线传感器网络程序。Avrora 是基于 ATEMU 的。ATEMU 是第一个指令级别的模拟器，它可以非常精确地模拟单个结点每个时钟周期的操作，但是不能适应大规模结点。Avrora 一方面与 ATEMU 一样是一个指令级别的模拟器，可以精确到时钟周期；另一方面又可以适应大规模结点，达到接近 TOSSIM 的执行效率。TOSSIM 和 ATEMU 是用 C 语言实现的，Avrora 则完全是用 Java 实

现的，所以 Avrora 具有很好的灵活性和可移植性。Avrora 和 ATEMU 因为模拟机器码而不依赖于具体的语言和操作系统，相反 TOSSIM 只能模拟 TinyOS 程序。

NS22 是现在无线传感器网络研究领域最流行的网络仿真软件之一，许多著名的协议如 LEACH、S2MAC 都是用 NS22 仿真的，其仿真结果具有一定的权威性。因为国内对 NS22 已经做了大量的研究，所以本文不再对 NS22 作进一步的介绍，这里只是对使用 NS22 仿真无线传感器网络程序和协议进行讨论。

RICE 大学的 Monarch 工程小组在 NS22 中添加了对无线和移动网络的支持，他们为无线网络的模拟提供了许多有用的组件，如无线信号传播模型、IEEE 802. 11 MAC 协议、移动模型。相对于 TOSSIM 和 Avrora 所提供的简单的外部通信模型，NS22 有能力提供一个复杂的、更接近于真实环境的网络通信模型。例如可以用 NS22 中的 OTcl 和 C++ 编写一个根据结点的物理拓扑结构和距离来设定物理信道通信失误率的通信模型。如果想验证一个新的无线传感器网络的路由算法或 MAC 层协议，那么 NS22 比 TOSSIM 和 Avrora 更合适。但是 NS22 只是一个网络模拟器，而不是一个代码模拟器，其工作重心在于网络通信模拟，对于结点的内部操作只提供了一个模型，而不是真正的执行代码，这就是它与 TOSSIM 和 Avrora 的区别所在。所以 NS22 不适合用来模拟无线传感器网络应用程序，却更适合模拟那些有着严格层次关系的协议，如 TCP/IP 协议。而在无线传感器网络中往往没有如此严格的层次关系，协议之间经常有跨层操作，应用程序层和协议层经常是互相影响的，如依赖于时间的数据融合操作、发送能量的动态调整操作等。所以 NS22 并不适合模拟所有的无线传感器网络协议，它的使用受到了一定的限制，需要在模拟之前分析清楚。但熟悉 NS22 并熟练应用其进行网络协议仿真并不是一件容易的事。

（2）其他仿真模拟器

SensorSim 构建在 NS22 的 802.11 网络模型之上。用户可以使用 SensorWare Tcl 脚本语言来编写程序。SensorSim 的目标平台是 WINS 平台，而不是常见的 Mica 平台。EmStar 为运行 Linux 操作系统的 iPAQ 和 Crossbow Star2gate 类型的结点提供了一个非常灵活的模拟环境，可以在模拟环境与实际部署环境之间进行切换。TOSSF 借鉴了 TOSSIM 中的许多设计思想，只不过它是把 TinyOS 程序的代码编译进了 SWAN 框架，它可以用来模拟异构网络。TOSSF 对结点间的通信只是提供了一个理想化的模型，甚至还不如 TOSSIM 的通信模型精确。OPNET 是由 OPNET Technologies 开发的网络建模和模拟工具，与 NS22 的功能基本类似，它有着与 Internet 相对应的严格的网络层次模型。Ptolemy 是 UC Berkeley 大学正在研究的一个项目，已经在 TinyOS 社区上发布了几个测试版本，其中的 VisualSense 就是一个无线传感器网络的建模和模拟框架，它支持无线传感器网络程序的设计、模拟及实时演示。

对业界公认的优秀专用网络仿真分析软件的应用过程，实际上也是学习规范化的网络

性能仿真、分析方法的过程。应用专用软件，尽管更多的是去学习和熟悉软件提供的仿真建模、验模方法，但只有对网络性能的评价方法、影响网络性能的因素、排队论、概率论、计算机仿真原理等有所了解，才能较好地应用专用软件。且了解越深，应用越自如，对仿真结果的分析越透彻，效果越好。有多种数学工具可以帮助对建立的模型进行必要的分析研究，比如排队论、Petri 网的运用等。

1）基于排队论的建模分析法。

排队论的建模方法在研究一个系统对一群体提供某种服务时很有用。在实际建模中，可以在对网络负载的性质及网络的运行做了一系列假定后，对系统进行大量地简化。用解析法分析网络大多基于独立性假设条件，各个结点的工作都是独立的、互不相关的，报文的到达时间和报文长度也是不相关的。解析法适用于具有单级排队系统的网络，可以进行一些静态的分析。对于复杂的、队列比较多且队列之间交互比较复杂的网络来说，用解析法来分析网络并得出公式比较复杂。

2）基于 Petri 网的建模分析法。

Petri 网是一种系统模拟与系统分析的有力工具，它可以比较方便地描述和研究具有异步、并行、频率和具有非确定性信息的系统。随机 Petri 网是在保留了基本 Petri 网模型结构和表示方法的基础上，通过引入时间的概念而逐步发展起来的，其目标是将形式化的描述、正确性验证和性能评价集成起来，是计算机网络性能评价中具有吸引力和改进性的数学工具。

3）模拟仿真法。

模拟仿真法就是编制一个程序对所要研究网络的全部或部分行为进行仿真，然后运行该程序，在程序的运行过程中采集数据，最后对该程序的运行结果进行统计分析。但对于网络仿真，如果对所研究的网络系统行为有一个详细的仿真，那将会得到一个比用分析法更为精确的数值，而且网络仿真可以检测到不同的因素对性能的影响。当然，和现实相比仍会有一定的误差，更何况网络仿真是通过模拟网络系统的行为来评价性能的，因此，可以评价网络系统的瞬间行为。但仿真方法的计算量太大，没有解析法简单明了，如果仿真模型不正确，那么得出的结果和现实将大相径庭。在分析研究网络系统性能上使用模拟仿真法，首要的是必须对仿真模型进行仔细的推理和验证，确定是完全正确后方能继续进行分析。

4）测试监控法。

所谓测试监控法就是直接对实际运行中的网络系统的各种性能指标或与之相关的量进行直接的测试，从而对网络系统的性能进行评价的方法。为了使测试值具有代表性，可以选择网络系统在比较接近通常条件的正常运行期间进行测试，例如要测试负载条件下的性能，就应该选择在每天网络最繁忙的时间内进行测试。

在测试监控过程中要注意以下几点：

① 必须根据研究的目的决定要测试的参数设置。

② 选择合适的测试方式和工具。测试的方式有两种：一种称为采样方式或外驱动方式，每隔一定时间间隔Δt，就对网络的一些参数进行一次测试；另一种称为事件跟踪方式或内驱动方式，就是先规定一些事件，以后每当网络中出现这些事件时就进行一次测试。常用的测试工具又可分为硬件测试工具、软件测试工具和混合型测试工具。选择测试工具时要注意工具本身的干扰性，因为用测试工具去测试系统时，一般会给系统的运行带来影响，造成系统性能的下降和测试结果的不精确，这一点对于软件测试工具特别重要。

③ 整个测试工作的实验设计、数据收集和处理方案及整个工作所需经费的估计。如果测试结果能真正反映系统的真实情况，实现的实验设计和事后的数据处理及解释都将非常重要。

测试监控法要在网络建立好之后才可以进行，绝大多数情况下，这不是一种切实可行的方法，因为有的网络太大、花费昂贵，不可能先建立起网络再确定其性能。

以上几种网络系统性能分析研究方法都具有客观性和实用性，有很强的应用价值，但网络系统性能评价是一个大工程，需要在实践中不断进行补充和改进。

6.5 典型系统应用案例

基于无线传感器网络的定位技术，设计了一个人群异常活动视频监控系统。该系统能够更精确地定位工作人员的位置，异常活动时能自动触发报警，只需要工作人员接到报警信息后赶到处理现场，从而提高了工作的效率。

系统由底层（硬件层）、中间层（串口消息解析层）、上层（数据处理层）系统构成，如图 6-5 所示。

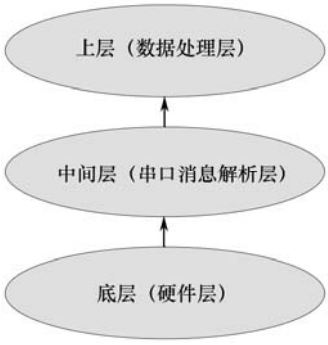


图 6-5　系统架构

底层模块通过 Move 结点发送数据到 Node1、Node2、Node3 结点，Node1、Node2、Node3 结点分别从 Move 结点中取出 RSSI 值并将这些值连同自身的 SOURECE_ADDRESS 值封装到数据字段并通过 Forward 结点转发给 Sink 无线网关结点。底层模块结构如图 6-6 所示。

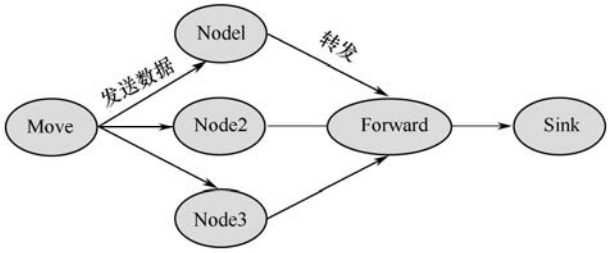


图 6-6　底层模块结构

中间层主要负责接收来自底层的串口消息，该层的重点就是对串口数据包的内容进行解析，获取数据包中结点的 RSSI 值、锚结点 ID 号等信息，并将其交给上层进行处理。

上层模块分为以下六个子模块。

串行配置模块：该模块为串口配置参数，为不同的网关配置不同的串行，使得系统的可扩展性增强。

实时监控模块：该模块主要负责将无线传感网络中移动结点的轨迹信息实时显示在监控画面当中，用户通过点击显示样例轨迹了解轨迹的概念，通过清除轨迹操作清除屏幕上的所有轨迹信息。此外，用户可以通过调整显示刷新周期，对轨迹数据的动态刷新周期进行设置。如果刷新周期设置过长，则通过手动刷新按钮刷新轨迹以实时观察移动结点的估计信息。

历史回放模块：该模块主要根据用户的设置回放移动结点的历史轨迹。用户根据自己的要求回放具体时间移动结点的轨迹信息，如回放一天、一天的一段时间，几天、几天里面的一段时间或者一个精确时间点的被监控人员的轨迹信息。此外，该模块提供设置回放周期功能，用户根据自己的需求设置每次回放的移动结点位置信息的个数和回放周期，系统将反馈给用户查询的时间段内数据库中所有记录的条数，用户通过系统能清楚地知道需要回放的记录条数以及待回放的记录条数。

历史数据查询模块：该模块主要负责历史数据的查询功能，模块包括人员位置/轨迹一般查询、人员位置/轨迹高级查询、历史警报信息查询三大功能。其中，人员位置/轨迹高级查询主要根据用户输入的时间段信息查询人员的轨迹信息，用户根据需求查询一天、一天的一段时间、几天、几天的一段时间或者是一个精确时间点的轨迹信息。此外，该部分还提供了一些其他功能，如用户在显示轨迹区域单击一个点，该单击点的在绘图区域的坐标、

该坐标对应的实际区域中的坐标及查询人员在该实际坐标出现的次数都将被列出来显示。历史数据查询模块的另外一个重要功能就是历史警报信息的查询功能。该功能允许用户查看所有的警报信息，即被监测人员所出现的所有非安全区域的信息。此外，系统提供用户根据需要删除部分选定的警报信息的功能。

非安全域设置模块：该模块主要负责非安全域的设置。非安全域的正确设置对系统的自动报警功能及系统的可靠性起着极其重要的作用。所以只有拥有设置权限的用户才能进行非安全域的设置。如果被监控的人员出现在非安全区域，系统将触发警报。非安全域即定义一个非安全域的中心和非安全域的半径，所有处在该非安全域中的点将触发报警功能。该模块允许拥有权限的用户根据实际需要对非安全域进行修改、添加、删除和查询等操作。

人员信息指南模块：该模块主要实现了对历史数据的统计工作。用户根据需求查询指定区域内出现的时间，此外，该模块还提供查询指定时间内被监控人员出现区域的功能。在指定区域出现的时间查询窗体中，用户设置需查询的区域或者根据输入的要查询的时间段，查询结果将显示所有查询到的记录条数，此外，该部分还提供了其他的一些功能，如用户可以获得被监控人员每个小时时段出现的次数以及每个小时时段在每天的 24 小时中所占的比例，这样根据查询的结果用户很容易获取在指定区域被监控的人员出现的最频繁的时间。在指定时间内位置信息查询功能中，用户输入要查询的时间段，得到查询结果后，用户单击任意一条查询结果，就可获取该单击点对应时刻和对应地点被监控人员出现的次数。

报警并录制现场模块：该模块提供报警和对现场进行录像功能，系统在发现人员出现在非安全域时自动触发报警并对现场进行一段时间的录像操作。此外，系统还提供解除警报或结束现场录制的功能。

本系统需要使用摄像头、micaz 结点及无线网关。无线网关与 PC 机通过串口连接，micaz 结点之间通过无线方式进行相互之间的通信，摄像头负责对现场进行录像。

第 7 章　传感网与物联网的服务、管理与应用

7.1　传感网服务质量与评价原则

无线传感器网络的服务质量技术是当前无线传感器网络研究的一个热点。在无线传感器网络的某些应用中，必须考虑网络系统服务质量的支持问题，如定位、探测和识别一个移动目标时需要用到的图像/视频传感器。传感器结点和控制者之间需要进行实时的数据交换，以便正确采取相应行动。因此，保证服务质量证是一个不容忽视的问题。

7.1.1　服务质量

（1）服务质量

这里的服务质量是指网络的通信质量，在有线网络中，通常是通过资源的超额供应或网络流量控制来获得服务质量技术的支持。由于所有的用户都在一个服务等级，在流量达到高峰时，服务可能变得不可预测。而在基于流量控制的方式中，业务可分成不同的服务等级，每个等级有不同的优先级。

控制服务质量最基本的方法是流量控制，即基于预留的方式和非预留的方式实现对服务质量的控制。基于预留的方式依据带宽管理策略以及业务的需服务质量要求来分配网络资源，如因特网的集成服务模型。基于资源预留的集成服务对网络中路由器的存储能力和处理能力要求都很高，但其占用的开销大，可扩展性很差。而非预留的方式无需预留网络资源，通过一些策略如接纳控制、策略配置、流量分类、队列机制等来获得服务质量。接纳控制机制负责在结点流量的入口处控制流量能否接入网络，并且保证被允许接入网络的流量的服务质量需求；策略配置确保没有结点违反预先为其分配的服务等级；流量分类区

分数据包的优先级并由此获得在每个中间结点上每一跳的具体行为；队列机制负责在发生拥塞时丢弃低优先级的数据包。

在无线网络中，如一个通信单元从一个基站跳到另一个基站，服务质量就可能由于新基站的带宽的不足而遭到限制，这些相关的技术和问题与有线环境是很相近的。但可将有线网络中的对多媒体信息存取的服务质量要求和无线多媒体存取质量控制协议结合起来。无线多媒体信息存取控制协议提供不同等级的数据流量，以不同的优先权接入共享无线媒介，从而获得系统整体的服务质量支持。虽然有基础设施支持的移动网络可以通过基础设施如基站和中心结点进行集中控制和管理，但如何实现基础设施之间的平滑切换和移动主机的无缝通信是其面临的主要技术难点。目前已提出包括小区切换机制和移动 IP 在内的大量协议和相关技术。

（2）特设网的服务质量技术

无线特设网络是一个移动的自组织多跳网络。随着信息技术的迅速发展，多媒体应用的不断开展以及与其他网络进行互联的需求不断增加，人们自然要求在特设网络上能够传送综合业务，并希望能像固定的有线网络或蜂窝无线网络一样为不同业务的服务质量提供保障。无线特设网络与传统有线网络和有基础设施支持的移动网络不同，它的网络拓扑经常发生变化，带宽、能量和存储计算能力受限。因此，原本在有线网络中运用的没有考虑移动性的服务质量支持机制和许多无线网络中没有考虑多跳情况的服务质量保障机制都无法直接应用。特设网络中的服务质量保证是个复杂的系统性问题，它意味着需要提供质量可以接收的信道，支持服务质量的信道接入协议，识别能满足业务量要求的转发结点及在结点实施拥塞控制和管理。

关于服务质量的定义，ITU-T 标准化组织在 E.800 中将其叙述为“服务质量是一种服务性能的综合体现，这种服务性能决定了网络在多大程度上满足业务用户的要求”。系统服务质量模型中保障机制的体系结构定义了网络中为用户提供的各种业务的质量标准和等级，标志最终应该达到的系统设计目标。系统服务质量模型影响着服务质量其他构成部分的功能，如网络只需提供分区服务时，就不再需要每个业务流状态的信令。服务质量信令是业务服务质量的控制中心，包括当前网络无线资源信息的收集、计算、分配、预留和释放，各个用户间业务请求的应答、调度等功能，同时协调服务质量 QOS-MAC 和服务质量路由算法。对多媒体存取的服务质量算法则根据协议确定的数据传输任务，完成相邻结点间的最终数据传递。它能否高效地使用无线信道是上层各种协议和机制所提供的服务质量能否得到最终保障的一个关键因素。

在无线传感网中，由于传感器结点的能源十分有限，如果结点因能量很快耗尽而失效或者网络中各结点能耗不均衡，就容易使网络中出现感知黑洞，甚至极大地缩短网络生命周期。所以，在设计无线传感器网络时，首先要考虑如何节能的问题，即网络能量有效使用问题。但在某些类型的传感器网络应用中，必须重点考虑服务质量支持的问题。服务质

量不仅在传统的电信领域里得到了广泛使用，还逐渐扩展应用于基于分组的宽带、无线和多媒体等服务领域。与此同时，通信网络和通信系统的设计和规划也越来越多地考虑到用户应用端到端的性能需求。服务质量是指网络为用户提供的一组可以测量的预定义的服务参数，包括时延、时延抖动、带宽和分组丢失率等，也可看成用户和网络达成的需要双方遵守的协定。服务质量也指网络对业务性能要求的支持能力。这里的性能要求是特定于不同业务的，如 IP 电话要求有尽可能小的抖动和时延性能，而远程医疗则需注重业务提交的准确性与重要性。

（3）无线传感网服务质量

无线传感网是一种无线自组织网，但又与传统的网络有一定的区别。其主要原因有两点：一是其采用的网络器件是微型传感器，这些传感器结点的能量、处理能力和容量都十分有限，同时结点密集分布在偏远恶劣的环境中，结点失效和因节能休眠会带来复杂且动态的拓扑；二是网络中的业务需要的并不仅仅是通信，还涉及感知信息的采集及产生、数据的协同处理以及信息的网内存储和直接转发等。随然只有这两个小的区别，但也给无线传感网中的服务质量支持增加了难度。

无线传感网中的需求服务质量与工作要求有关，不同业务对于服务质量有着不同的要求和解释。因此直观上可以定义激活的传感器的覆盖范围或者数量作为衡量无线传感器网络中服务质量的参数。或者，上述错误也可能来自传感器的功能受限，如观测精度的不足或数据传输速率较低。因此也可以定义观测精度或是测量误差作为衡量服务质量的标准。

一些要素的考虑和相关设备的选取对系统的工作质量有着直接的影响。包括一些典型参数，如传感器的覆盖范围、传感器位置排列、测量误差以及激活传感器的最佳数量等。同时任务对传感器的布置、激活传感器的数量、传感器的测量精度等都有特定的要求，因此，针对指定的业务和工作内容，必须注意任务要求和相关参数的配置。

考虑基础通信网络怎样才能传输服务质量感知数据，并且能够有效地利用网络资源。虽然不可能分析无线传感器网络中所有设想的业务，但可以根据不同的数据传输模式来分析各个不同类型的业务，因为每种类型中的大部分业务都有共同的需求。在无线传感器网络中，受关心的是数据怎样传输给汇聚点以及由业务特性所决定的相应的一些处理和传输的需求。

在无线传感网应用中，如环境监测、目标视频跟踪和分布式存储等的服务质量（QOS）需求。应用层的 QOS 需求，如系统寿命、响应时间、数据更新度、检测概率、数据保真度和数据精度等是由用户指定的。需要网络设计者来平衡和调节，在给定相同的物理层射频 RF 单元，在 MAC 改善传输可靠性的同时会恶化有效节能，因为它带来了重传、确认以及纠错编码等能量开销。无线传感器网络与应用相关的需求还有覆盖、暴露、测量差错及最优激活的结点数目等。与网络相关的服务质量的需求要注意解决以下几个问题：

1）底层的网络如何有效地利用网络资源传输服务质量约束服务质量的传感器数据。

2）通过数据传输模型分析每一类应用。

3）选择数据传输的模型，如事件驱动、查询驱动及连续传输模型等。

注意到无线传感器网络与传统数据网络需求的差别：无线传感器网络不再是端到端的应用，因此，服务质量是集体参数，如集体延迟、集体分组丢失、集体带宽以及信息的吞吐率等；带宽并非是单个传感器结点主要关注的目标，或许一群传感器结点才会关注带宽；可以容忍单个结点产生的业务分组丢失到一定程度；大多数无线传感器网络应用都是任务紧急的应用，对延迟有较高要求。

（4）无线传感器网络服务质量特点

根据使用含义的不同，服务质量可以从两个不同的视角来解释。从用户角度来说，服务质量指用户所感知的业务的服务质量水平，用户并不关心网络内部设计的细节问题，他们只关心最终能够获得的网络服务质量；而从网络角度来说，服务质量是网络提供给用户的服务质量水平量度。网络的目标是在提供服务质量的同时，最大化利用网络的资源，即获得更加确定的通信行为，以便能够更加安全可靠地保护网络承载的信息，并更加高效地使用网络资源。为了达到这个目标，网络必须能分析各种应用需求并采用相应的服务质量机制。网络提供特定服务质量的能力依赖于网络自身及其采用的网络协议的特性。对于传输链路而言，包括链路时延、吞吐量、丢失率和出错率；对于网络结点而言，包括处理速率和内存空间等。此外，运行在网络各层的各种服务质量控制算法也会影响网络的支持服务质量能力。

（5）事件驱动模型

当网络监测到某一事件发生时，目标附近的结点将立即处于激活状态，将采集到的数据传送给 Sink 以便通告最终用户，如针对某幢大楼化学元素释放的紧急事件进行感知和反应，事件驱动模型的需服务质量求有以下特点：

1）应用程序本身并不是端到端的，具体地说，应用程序的一端是 Sink，但另一端并非单个传感器结点，而是受事件影响的某一区域内的若干传感器结点。

2）来自这些传感器结点的数据很可能具有高度关联性，因此包含大量的需要整理提取的冗余信息。虽然由单个结点发出的数据流量强度可能非常低，但是事件突发时，大量的结点将产生突发的大流量，网络要保障流量的可达性。

3）一旦侦查到事件，应用程序必须尽快且可靠地做出恰当的反应，因此其对实时性要求较高。

4）模型的应用必须是可交互的，要求重要信息具有较高的可靠性。

查询驱动模型：在查询型网络应用中，首先由应用程序或者终端用户发出感兴趣的查询消息，之后，传感器结点将符合查询条件的数据逐跳转发至 Sink 结点。

查询驱动模型与事件驱动模型的区别在于：前者是通过 Sink 来请求数据，而后者是传感器结点主动将数据发送给 Sink。这里所提到的“查询”也可能包含针对传感器结点的配置和管理信息。如果 Sink 想升级传感器结点的软件，重新配置发送速率，或者改变结点的任务，则 Sink 可发送一个指令来执行这些任务。

连续传输模型：在连续传输模型中，结点不断采集数据，并以预先设定好的速率向 Sink 发送数据。该模型的数据包括实时和非实时两种。实时的数据包括语音、图像和视频等。而非实时的数据可能是 Sink 在一定区域内周期性收集的数据。

在连续传输模型是非端到端的程序中，关键性是非交互性。此外，不同的数据类型也有不同的服务质量需求：实时的数据受限于时延，且有确定的带宽需求；非实时的数据可以容许一定的时延和数据包丢失。

无线传感器网络是与应用相关的网络，这种同应用相关的设计方式的优点是能够对网络和结点软硬件资源，根据不同应用的要求最大限度地进行优化；缺点在于网络软件、硬件、拓扑、结构和路由等，在不同应用下有不同的表现形式，每种服务质量应用对应的要求也不尽相同。

由各类型对不同性能的要求可以看出，无线传感器网络所保障的服务质量不再是传统网络中端到端的概念。带宽和丢包率不再是单个传感器结点所关注的主要目标，而是在特定时刻内一组传感器结点突发性传输数据所必需的服务质量，这种保障强调以任务的关键性为中心。

混合型：在很多应用中，上述数据传输模式同时存在于网络中。因此，需要有一个机制来适应有不同限制服务质量的流量类型。

由表 7-1 还可看出，无线传感器网络中的业务需求和传统网络有许多不同。首先，传感器网络中的大多数业务不再是传统的端到端业务。其次，对于单个传感器结点，带宽并不是主要关心的，但对于一组传感器结点在某个特定的时间周期内，带宽是需要着重考虑的，这归结于传感器流量的突发特性。因为冗余数据的存在，所以允许流量中有一个由传感器结点产生的特定程度的丢包率。最后，无线传感器网络中的很多业务都是重要业务，都有很高的优先级。

表 7-1　不同数据发送模型的性能需求

业 务 种 类	基于事件驱动	基于查询驱动	基于连续驱动
端到端（End-to-End）	否	否	否
交互性（Interactive）	需要	需要	需要
有限时延（Characteristics）	不容许	具体设定	容许
任务的关键性（Criticality）	是	是	是

无线传感网服务质量和用户的信息服务质量的交互是一种模型，网络为用户提供支持，而用户给网络提出需求。由于网络体系结构中每个层次都有不同的需求服务质量，如 MAC 层需服务质量需要物理层提供信道的信噪比以确定选择由哪个质量较佳的信道进行用户接入和传输。网络层需要 MAC 提供信道的使用情况，以决定选择哪条业务最不拥塞的路径路由数据。传输层也需要网络和 MAC 层的状态信息，以便满足用户对传输差错率的要求。因此，根据用户具体应用的不同，恰当地选择合适的保证服务质量机制，是无线传感器网络保证服务质量技术未来研究的主要课题。

在设计无线传感网保证服务质量机制时，不但要考虑来自用户应用的需求，还要对系统网络的特点和结构做深入的分析。表 7-2 给出了设计无线传感器网络保证服务质量机制应当考虑的主要因素。此外，在处理无线传感器网络的业务时，还应该注意以下几个方面：网络带宽的限制、消除冗余数据传输、能量和延迟的平衡、点缓存服务质量大小的限制和多业务类型的支持。

表 7-2　服务质量保证要素

问　　题	考虑的主要因素
网络的动态变化	包括传感器结点、目标跟踪和 Sink 结点的移动性
数据传输模型	连续模型、事件驱动模型、查询驱动模型、混合传输模型
数据汇聚、融合	在网内（部分或完全方式）或网外汇聚或融合处理
结点通信	单跳、多跳、单跳–多跳相结合
结点功能	多种或单一功能，同构或异构功能
结点部署、配置	按照预先规划的或以 AdHoc 自组织方式

无线传感网的服务质量通常定义为传感网平均精度，即向信息收集的汇聚结点发送信息的最优的传感结点数目。如网络结点数过少，不能保证传感结点采集信息的精度；又如结点数目太多，又不能实现最小化能量的使用。其基本工作方式是广播原理，即信道将服务质量信息发送给每个传感结点，并运用一个称为 GurGame 的数学优化方法，来动态调节最优的传感器数目。动态调节来自传感结点的服务精度。

7.1.2　无线传感网的服务质量

（1）服务类型

主要有两大类：集成服务类型和区分服务类型。集成服务是指在整个网中，为某一业务流量保留一定的带宽，为该业务提供一条端到端的透明通道。基本思想是在传送数据之前，根据业务需求进行网络资源预留，从而为数据流提供端到端的服务质量保证。该服务能够在 IP 网上提供端到端的保证，但集成服务对路由器的要求很高，当网络中的数据流数

量很大时，将受到来自路由器的存储和处理能力的限制。因此，集成服务可扩展性较差，难以在因特网服务质量核心网络实施。区分服务定义了一种可以在互联网上实施的可扩展的服务分类，是一种基于每一跳的策略。区分服务的基本思想是将用户的数据流按照服务质量要求来划分等级，任何用户的数据流都可以自由进入网络。当网络出现拥塞时，级别高的数据流有更高的优先权。区分服务只承诺相对的服务质量，而不对任何用户承诺具体的服务质量指标。因此区分服务模型和集成服务模型由于其自身的复杂性经常不适用于无线传感网，而跨层结构比分层结构更有助于设计出简单的传感网模型。

（2）服务质量算法

服务质量算法有很多，可以基于流量类型、数据传输模式、传感器类型、应用业务类型以及包的容量。关键在于如何根据业务需要合理地进行流量区分，如何控制不同类型流量的网络资源分配以获得最大的资源利用。

服务质量集成与度量和服务体系需要研究怎样将无线传感器网络和基于 IP 的网络综合起来。如许多业务服务质量需要从传感器结点收集数据并传送到因特网中的一个服务器，以开展进一步的分析，或者用户会通过因特网来向 Sink 结点提出请求，需要研究如何让同时运行于两种网络之上的业务获得服务的无缝结合。以数据为中心、面向应用的传感器网络以非端到端数据传输为主，需要体现一对多、多对一或多对多的通信模式。

关于实时、可靠和自适应的服务质量问题，传感器网络高度冗余的数据可提高数据传输的可靠性，但会消耗过多的能量。存储资源数据融合可有效减少数据冗余并节省能量，但又会增加传输延迟。通过理论分析或者仿真试验寻找一种最优的自适应服务质量平衡机制非常重要。结点活动性调度是节约网络能耗和延长网络生存周期的有效办法。

（3）跨层优化

无线链路在衰落、干扰和噪声等因素作用下信道质量的波动，能量控制策略下结点工作状态的转变，结点增减或移动带来的网络拓扑变化，都需把物理层的信号质量及时通知 MAC 层，MAC 层也需要及时和网络层、传输层以及应用层进行信息交互。传统分层协议体系体现了“开放”和“互联”，但在面向应用且资源受限的传感器网络中并不是最优的方式。考虑网络各层间的相关性，实施基于跨层优化的服务质量机制，可以最大限度利用有限资源，并在效率、开销、可靠性和可扩展方面求得平衡。

1）数据传播与服务质量控制机制。该机制包括协议是否具有优先级，当超负荷或在一个高动态的网络中网络能否发送具有高优先级的数据等。还包括无线传感器网络能提供什么样的非端到端服务，传统的尽最大努力、有保证的、区分的服务能否在新的条件下适用等。传感器有时会过度地发送一些数据，有时也会发送一些不充分的数据，既达不到应用的要求，又浪费了宝贵的能源。因此，需要一些集中式或分布式的服务质量控制机制。

2）端到端、能量与聚合性服务质量参数的支持。尽管在无线传感器网络中这些不是主

要关心的，但在某些情况下它们仍可以使用，而且在某些极端的情况下研究服务质量的局限性是很有意义的。

利用聚合性服务质量参数为 3 种数据传输模式提供一些支持是很有意义的，需要研究的是怎样区分这样的机制与传统网络的机制。

无线传感器网络的数据冗余性可以极大地提高信息的可靠性，然而它消耗极大的能源来传输这些数据。若引入数据融合技术，则可以有效降低数据冗余性，提高能源利用率，但可能导致时延。通常采用折中的服务质量方案可能得到较理想的系统特性。

7.1.3　服务质量保障

无线传感网的服务质量目前还没有统一的参数度量体系和标准。有人提出非端到端，即网络所要保证的不是 Sink 与单个传感器结点的端到端之间的服务质量，而是由应用所决定的 Sink 同“一组”或“多个”传感器结点之间的服务质量。即当某事件触发后，监测区域内的一组传感器结点将由休眠状态转变为激活状态，进行感知任务并向 Sink 结点传输采集到的数据。

由此可见，传统的网络服务质量参数不足以度量无线传感器网络的服务质量的需求，需要定义一些新的服务质量参数，对网络性能进行有效的评价，统称为聚合的服务质量参数。

聚合性时延：监测到事件发生后传感器结点产生的第一个数据包与最后一个到达 Sink 的数据包之间的时间差。

聚合性丢包率：在传递过程中与监测事件相关的数据包丢失的数量，而不是单个结点的丢包率。

聚合性带宽：位于监测区域内的传感器结点向 Sink 结点传输数据所需要的总带宽。

信息吞吐量：Sink 结点与监测区域内传感器结点之间的总吞吐量。

由上述指标可知，这种非端到端的服务质量性能指标已不同于传统 IP 网络中端到端的服务质量度量指标。非端到端的概念所针对的是无线传感器网络面向以数据为中心的应用，把应用所决定的任务交给一组传感器结点来执行，即将网络层面的服务量问题映射到结点层面来解决。结点层面的服务质量所要保证的是 Sink 结点与执行任务的多个传感器结点之间的性能指标是否满足服务质量的要求，而不是针对具体的某个传感器结点。

（1）跨层服务与质量保障

关于无线传感器网络中服务质量的研究以往基本上是孤立的，或是特定在某些功能层上的研究，或是特别指定某些应用场景的研究。跨层设计是通过层与层之间的信息共享及交换来满足全局的、整体的需要，是对网络进行的整体设计和全局的优化。它模糊了严格的层间界限，将分散在网络各子层的特性参数协调融合，通过信息交互，可以以全局的方式适应特定应用所需的服务质量和网络实际状况的变化，同时可以根据系统的约束条件和

网络特性来进行综合优化，实现对网络资源的有效分配，提高网络的综合性能。可以看出，跨层的设计方法对无线传感器网络来说非常适合。例如，在无线传感器网络的某些应用中，需要网络的生存时间足够长，而时延要尽量短，这对于传感器网络能量有限供应和受限的结点资源与带宽来说是矛盾的，因此，有必要在紧密联系的各功能层之间引入跨层设计的思想。

1）无线传感网的服务质量框架。网络体系结构是网络的协议分层，是对网络及其组成部件所应完成功能的定义和描述。而无线传感器网络的网络体系结构是不同于传统网络的，有着其特殊的功能层。表 7-3 所列的无线传感器网络参考体系结构表示将无线传感器网络的一系列功能分解到各个功能层上，以便随后在不同层次上进行服务质量网络性能参数的映射。

表 7-3　无线传感器网络参考体系结构

<table>
<tr><td colspan="4">应用层（事件驱动型业务、查询驱动型业务、连续型业务、混合型业务）</td></tr>
<tr><td>数据管理层</td><td rowspan="4">拓扑维护</td><td rowspan="4">覆盖维护</td><td rowspan="4">结点定位时钟</td></tr>
<tr><td>传输层</td></tr>
<tr><td>网络层</td></tr>
<tr><td>MAC 层</td></tr>
<tr><td colspan="4">物理层（感知能力、处理能力、通信能力）</td></tr>
</table>

在表 7-3 所列无线传感网的网络体系结构中，有 1 个水平层的数据管理层和 3 个垂直层的拓扑维护、覆盖维护、结点定位和时钟同步，是无线传感器网络的特殊功能层。无线传感器网络的网络体系结构中最上面是应用层。无线传感器网络的业务可分为事件驱动型业务、查询驱动型业务、连续型业务和混合型业务。数据管理层提供数据的存储转发、网内处理等功能。从传输层到物理层类似于传统网络的通信协议栈，但运行于高度动态和资源受限的无线传感器网络环境中。传输层负责源传感器结点与接收发送器之间感知数据的传输。网络层将感知数据分组从源传感器结点经选定路由传送至 Sink，同时也采用流量控制来避免拥塞。MAC 层提供传感器结点间在通信范围内的跳到跳的通信，该层还负责传输的调度和能量节省、忙闲周期问题。由于传感器结点工作状态的高度动态性（激活、休眠等），传感器的随机分布以及部署的高度密集性，需要一个拓扑维护层来维持网络的连通状态，覆盖维护层保证目标区域被最少但足够数量的传感器结点监视。无线传感器网络的用户要把感知数据和实际物理世界中的现象关联起来，所以，结点定位（允许传感器结点对自身定位）和时钟同步（保证传感器结点之间时间的一致性）服务层也是必要的。基础层（即物理层）指出了一个传感器在结点感知、计算和通信方面的物理能力。

应用层的服务质量一般是由用户选定，数据管理层一般指被网络传输和处理的真实比特，而信息是指已经获得的认知或是从数据中提取出来的结论。这里的数据管理层是指能

够理解“信息”的最低层，传输层的任务是为源端机到目的机提供可靠的数据传输。而在无线传感器网络的传输层中需要用到“聚合”的概念，只要是包含与已接收数据相关的数据分组都可以看成一个聚合，属于一个特殊的包；而只有包含与已接收到数据不相关的数据分组才能算另外一个聚合，属于另一个特殊包。物理层描述了无线传感器结点各方面的性能，即感知、处理和无线通信这三大组件的性能，包括测量精度、感知范围、感知功率。处理单元性能包括结点定位能力、时钟同步能力、处理速度以及计算能力。无线通信单元性能包括信道速率、编码和射频功率。

感知单元测量精度影响覆盖可靠性、覆盖鲁棒性，感知范围影响覆盖百分率。因此感知功率也影响覆盖维护层的所有服务重量需求；处理单元性能影响结点定位能力和时钟同步能力，分别影响向定位精确度和同步精确度；处理速度决定数据管理层的处理时延、计算能力，影响数据管理层的计算花费、数据抽象度和数据精确度。同时这些性能也影响结点定位/时钟同步层的服务能量消耗。

2）无线传感网服务质量。受相同低层服务质量需求影响，两个不同高层服务质量需求之间关系，大致有四种情况。

竞争关系：两个高层服务质量需求对低层所提供的有限的资源有着相同的要求。例如，给定数据管理层处理器的处理时延，要改善应用层的响应时间需要更多的 CPU 时间去处理查询信息。而要改善数据更新时间则需要更多的 CPU 时间处理感知数据。两者将竞争同一有限资源，即 CPU 时间。

对立关系：其中一个高层服务质量需求的提高需要低层服务质量需求的提高，而另一个高层服务质量需求的提高需要同样低层服务质量需求的降低。例如，提高 MAC 层的通信范围，需要物理层的射频功率更高，而要提高 MAC 层的能量效率，需要射频功率更低。

消长关系：在同一个低层服务质量需求水平下，改善高层服务质量需求中的一个会导致另一个服务质量需求的恶化。例如，在同样的拥塞概率下，提高数据传输的可靠性需要更多冗余数据包的传输，然而这样就增加了能量消耗。

协调关系：两个高层服务质量需求，对低层服务质量需求的要求可能是不同，既不竞争同一资源，也不是消长关系。例如，传输层的数据传输可靠性的提高可以使数据管理层的存储丢失率和提取丢失率同时改善，且给定数据传输可靠性后其两者是独立的，所以两者是协调关系。由此，两个高层服务质量需求之间只有符合前 3 种关系时才会存在一个权衡点，如在 MAC 层的通信范围和能量效率之间就存在着权衡点，但如果高层服务质量需求同时受几个低层需求的影响，那么就不能采用此种描述方法。连通性维护层的网络直径和网络容量同时都受 MAC 层通信范围的影响，通信范围越大越能改善网络直径。但是通信范围越大，导致邻结点之间的冲突越多，从而使得网络容量下降。网络直径和网络容量之间有一个权衡点，从而改善网络直径会使得网络层的路径时延改善，改善网络容量会使得网络层的拥塞概

率改善。所以，网络层的路径时延和拥塞概率之间也存在着一个权衡点。这些权衡关系的发现能够更加促进理解无线传感器网络系统中跨层之间的相互作用与影响。

3）服务质量的跨层设计。利用无线传感器网络参结构，可以进行如下跨层设计。

- 网络的每一个功能层把会对其他功能层产生影响的服务质量需求信息直接或间接地传递给相应的层次，如物理层的发射功率、测量精度，MAC 层的通信范围、网络层的拥塞概率等。
- 网络的每一个功能层分析从其他功能层传递过来的影响本层性能的服务质量需求信息，并对本层的通信做出相应的调整。例如，网络层根据拓扑维护层提供的拓扑状况和 MAC 层提供的链路状况实施路由协议，以实现最小路径时延和拥塞概率。
- 对于会影响到多个功能层的服务质量需求参数，要结合业务性能要求对各层进行综合考虑，对相关的性能参数进行折中考虑。如物理层的射频功率同时影响 MAC 层的通信范围和传输可靠性、拓扑维护层的网络直径和网络容量、网络层的路径时延和拥塞概率以及传输层的数据传输时延和数据传输可靠性。因此，在进行网络设计时就要充分考虑这些影响，在网络能量消耗、时延、可靠性之间进行有效折中考虑。

（2）中间件与质量保障

1）基于中间件的服务质量。主动服务质量机制建立在应用和网络协商的基础上，可对应用质量、网络结构或路由等进行主动调节与干预。中间件能实现应用与网络间的翻译和控制，支持两者协商新的 QOS。传感器网络的中间件技术的已有研究，更多的是集中在中间件问题本身，未上升到服务质量支持层面。因此，研究如何基于中间件实施主动服务质量机制值得关注。

服务质量对于网络来说用简单的方法是难以保障的，但采用通过网络之间的中间件进行协商（即设计一种中间适配层来适应下层网络和端系统资源的动态变化，它能够方便上下层之间的交互）使上层及时获取底层的反馈信息并使下层能够准确理解上层数据的语义和贯彻上层的决策，这样则可以提高系统的整体性能和应用感知的服务质量。

用中间件可以为无线传感器网络应用屏蔽掉底层平台的差异，应用和网络之间通过中间件的标准 API 接口交换信息。中间件为主动服务质量的协商和干预机制，提供了一个收集、分析与判断分散结点信息的合适平台，通过调整使网络能够最大限度地支持服务要求、延长网络生命周期。

2）服务质量动态管理。其设计思想是对允许的资源预留请求规定一个范围，网络在规定的范围内为应用提供服务，采用服务质量范围而不是单个固定值可以增加服务质量在请求范围内得到维护的概率，提供软服务质量保证，并在最大服务质量和最小服务质量之间动态调节应用的服务质量要求来适应网络资源的变化。在无线传感器网络中由于动态变化

的网络特性，不宜采用静态指配的资源管理方法，而应采用动态资源管理机制来保证资源分配的高效性。当经过协商后确定资源能够满足服务质量请求，则可为应用预留和分配所需的资源。否则，需要等待其他流释放资源或重新协商服务质量要求，系统可根据资源分配和可用资源变化，调节各业务流速率和占用资源的状态。动态资源管理的框图如图 7-1 所示，这种方法对于网络元素不稳定和整体资源受限的无线传感器网络来说是非常必要的。动态资源管理和基于中间件的服务质量技术是提供服务质量保障非常有效的方法，当网络对应用的支持发生变化后，需要通过动态调节的方式，使网络满足对应用的最低要求，或者在降低应用对服务质量要求的情况下，使网络最大限度地支持应用。

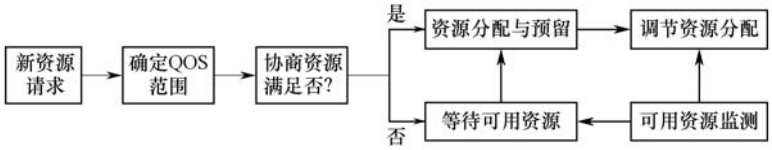


图 7-1　动态资源管理

3）实时业务的服务质量方法。建立从源结点到簇头的数据传输路径时，首先，要保证能量有效性；其次，计算结点之间的链路代价，主要考虑传输的花费、结点的剩余能量以及信道误码率等因素。在无线传感器网络的一个簇内，簇头结点负责收集来自簇内成员的数据。簇内采用多跳的通信方式，每个负责转发数据的结点对于来自源结点的数据需要进行分类和调度处理，将实时业务和尽力而为业务的数据通过分类器分配到不同队列中。定义带宽比例系数 r 来表示分别用于实时业务和尽力而为业务的带宽比例，根据比例的大小由调度器来决定不同业务种类分组的传输顺序。建立无线传感器网络的服务质量，虽然在不可靠的数据传输的基础之上，但并不排斥业务流的优先级表达式。当网络中同时具有实时业务和尽力而为的业务时，可以采取以下的方法来确保实时业务对于服务质量的要求。

7.2　传感网管理

无线传感网服务质量管理主要包括能源管理、覆盖机制、数据融合和拥塞控制 4 个方面。

1. 能源管理

无线传感器网的能量受限，在传感网中高效利用有限的资源，才有可能实现能源管理的高效，而且有助于实现无线传感器网络能量的平衡。传感器网络的能源管理可从低功耗设计、节能软件设计、无线通信、路由协议、网络优化、能量收集等几个方面入手。

1）低功耗设计可结合硬件和软件节电的电源设计。例如，选择低功耗的微控制单元

（MCU），选用较低的输出电压，尽量使用中断，减少收发模块的启动时间等。

2）在节能软件设计上，可对操作系统和应用程序接口进行优化。其中，动态电源控制和动态电压调整能使操作系统在性能和能耗控制之间进行折中；设计良好的应用程序接口API 应该清晰地注释出能量、质量、时延和操作点等，以便用户建立节能的系统。

3）在无线通信方面，有 3 种方式来降低能耗。随着传输数据的减少而降低调制等级，降低传输速度；随着通信距离增加，使用多跳短距离通信以减少单跳通信的距离；减少通信流量。

4）在路由协议设计方面，必须考虑均匀使用结点能量和数据融合两个方面。从整个网络来看，均匀使用结点能量是为了避免个别结点过早的耗尽，以致缺少某块区域的信息甚至网络瘫痪。而数据融合的作用是减少同一区域内结点数据的冗余性，从而有效降低整个网络的数据流量。

5）在 MAC 层协议的设计上，首要目的是延长网络系统的生存周期。现阶段对于 MAC 层协议的节能机制研究较为成熟，实现能源控制的措施包括：减少和避免信道访问冲突，利用周期性的监听和睡眠来减少空闲监听时间，避免串音，对大数据进行分段，控制发送功率等。此外，MAC 层协议的可升级性也很重要。

6）在整个网络的优化上，可从流量分发与拓扑管理两个角度来降低能耗：在流量分发方面，可在源和目的地之间寻找一条节能的多跳路由；在拓扑管理方面，可降低结点密度，利用较少的结点跟踪事件，从而减小计算的复杂度。

此外，还可通过降低发射功率来减少网络电源的开销。除了以上策略，能量收集技术的发展也使无电池但具有无限生命周期的无线传感器网络成为可能。能量收集即通过对环境中的机械振动，光能、电磁场、化学能、温度变化、风、热等能量进行收集、转换及存储，并分配到网络传感器的各个部件，从而保证电源需求，实现长期的有效供电。能量收集是无线传感器网络在节能方面的前沿热点技术。现阶段，对于机械振动和光能的能量收集技术已经较为成熟。

2. 覆盖控制

覆盖控制是指在结点能量、网络带宽、计算能力受限的情况下，对传感器结点进行合理放置，并采用适当的路出选择，使无线传感器网络的各种资源得到优化分配。覆盖控制不但提高了能量的有效性，节省网络资源，而且减少了数据的冗余，同时对网络的动态性和可扩展性也有一定的支持。典型覆盖控制算法与协议。

（1）基于网格的覆盖定位传感器配置算法

该算法通过采用网格形式来配置传感器结点以及目标点，传感器结点采用 0/1 覆盖模型，并使用能量矢量来表示格点的覆盖。其目标是在有限的代价条件下，使错误距离最小化，从而优化覆盖识别结果。

（2）轮换活跃/休眠结点的结点自调度覆盖协议

该协议建立在圆形二进制感知模型的基础上，采用结点轮换周期工作机制。在该协议中，每个周期包含一个自调度阶段和一个工作阶段。在自调度阶段里，各结点首先向传感半径内的邻居结点广播通告消息，然后分别判断自身的任务能否由邻居传感器来完成，从而决定进入“休眠状态”还是继续工作，这样便可有效减少网络中的信息冗余。但为了避免出现“盲点”，该协议需要采用一个退避机制以保证网络的充分覆盖。结点自调度覆盖协议不仅对结点冗余进行调度，而且通过结点轮换工作和休眠的机制来减少能源消耗，从而有效延长了网络的生存时间。

（3）最佳与最差情况覆盖

该算法考虑的是如何感应并追踪穿越网络的目标或其所在路径上的各点。最佳与最差情况覆盖着重从距离和某些特殊路径的角度来考察网络对目标的覆盖情况。该算法通过设置一定参数来计算无线传感器网络最佳和最差的覆盖情况，并计算出临界的网络路径规划结果。人们可以通过以上结果对网络结点的配置进行指导，从而改进整体网络的覆盖。

（4）暴露穿越

暴露覆盖模型更能符合一个实际情况，即目标穿越 WSNs 监视区域的时间越长，被检测到的概率就越大。在该算法中，根据不同的前提条件有不同的确定公式来计算暴露路径，其中最小暴露路径表示无线传感器网络最坏的覆盖情况。

3. 数据融合

无线传感器网络通过密集分布的大量传感器结点来收集信息。如果原始数据不加处理就直接传送给中心结点，将产生大量的数据冗余，这将给通信网络带来巨大的开销，大大消耗传感器结点的能量，从而减小网络的使用寿命。数据融合，即在每一轮的数据采集过程中，结点采集到的数据包先经过集中汇总，再传输到汇聚结点，这样可以减小数据传输到汇聚结点的次数，减少传感器结点和汇聚结点之间的传输量。可见，数据融合不仅能够减小数据冗余，而且有效节省了网络的能源。下面简单介绍三种典型的数据融合协议。

（1）直接传输法

在该协议中，所有传感器结点都把收集到的数据单独发送给汇聚结点后再进行融合。在直接传输法中，距汇聚结点较远的结点将较快耗尽能量，这容易导致整个网络能量分布很不均匀。除此之外，在很多情况下，数据产生的地点都具有局部性，因此集中进行数据融合的效率会低于局部信息融合。由此可见，直接传输法适用于传感器结点与汇聚结点比较近，且接收数据消耗的能量比传输数据消耗的能量大很多的网络。

（2）基于层次的 LEACH 协议

在该协议中，监视区域内结点通过自组织的方式构成少量的簇，由每个簇中指定的一个结点对簇内其他结点发送的数据进行收集与融合，并将融合结果发送给汇聚结点。在

LEACH 中，簇头的选择是随机的，因此每个结点都有机会成为簇头，其目的是为了平衡各个结点的能量消耗，从而避免网络能量分布不均的情况。该协议有效延长了网络的生存时间，并提高了数据传输效率。但应该注意到，LEACH 在节约能耗方面还未能做到最佳。

（3）PAGASIS 协议

该协议是在 LEACH 协议的基础上改进而来的，被认为无线传感器网络中接近于理想的数据采集方法。PAGASIS 的基本过程是：将监视区域内的传感器结点排列成一个链，每个结点都可从最近的邻居结点接收并发送数据。当一个结点接收到上一个结点的数据后，先将自己的数据和该数据进行融合，再将数据传送给下一个结点。最后，由一个指定的结点将融合结果传输给汇聚结点。通过 PAGASIS 协议，可以保证每个结点都将数据传输给汇聚结点，且大大降低了结点在每一轮数据传输中耗费的能量。

数据融合技术是无线传感器网络的关键技术之一。根据不同的应用需求以及网络特性，数据冗余情况有很大的差异，因此融合处理方式也有所不同，目前还没有统一的处理模式。

4．拥塞控制

在无线传感器网络中，不稳定的流量、多对一的通信和多跳的数据传输方式是造成网络拥塞的主要原因。此外，可能造成网络堵塞的还有感知事件之后的突发流量，拓扑结构的高度动态性，频繁变化的无线信道，不同信道上互相干扰的并发数据等。拥塞可能引起丢包率上升、时延增大、能源消耗增多，从而导致全局信道的质量下降。由于 WSNs 自身的特点，传统端到端网络的拥塞控制策略不适用于无线传感器网络。

拥塞控制可分为拥塞检测和拥塞减轻两个阶段。这里简单介绍一下在无线传感器网络研究中现有的几个拥塞控制策略：

（1）CoDA（Congestion Detection and Avoidance）

针对基于事件驱动的 WSNs 检测到事件引起的拥塞，CoDA 的机制包括基于接收端的拥塞检测，开环 Hop-by-Hop 的后压和闭环多源调节。该算法可调节局部造成的拥塞，并减少逐跳控制信息的能耗，但其中使用的速率调节方式会使距离 Sink 较近的源结点发送更多的分组。

（2）ESRT（Event-to-Sink Reliable Transport）

针对 Sink 结点只关心集合信息而不关心单个传感器结点信息的特点，ESRT 在拥塞监测上采用了基于结点的本地缓冲监测，并根据当前网络的状态进行结点速率的调节。该算法主要适用于 Sink 结点，它可减小网络能耗，提高可靠性，但不适合只发生短暂拥塞、大规模的网络。

（3）自适应的资源控制

该算法针对拥塞期间重要数据包可能丢失的情况，并假设网络中通常有空闲结点可供调度。算法通过创建多元路径对资源供应进行了自适应的调整。该算法采取了拥塞检测、

创建选择路径、多路通信三个步骤。自适应的资源控制增加了传送分组的精度并节约大量的能量，但多元路径热点距离过近可能引起冲突，而距离初始路径过远还可能增加分组传输延迟和能量消耗。

（4）Fusion

该算法结合了三种拥塞控制机制，分别是 Hop-by-Hop 流控制、源速率限制模式和有优先级的 MAC 层协议。三种机制的有机结合减小了信道丢失率，明显改善了网络的有效性和公平性。其弊端是速率限制模式无法杜绝隐终端冲突、歪斜路由、结点故障等问题。

（5）多到一路由的拥塞控制

针对无线传感器网络多到一的通信导致汇聚结点附件拥塞的问题，该算法通过确定下游孩子结点最小允许发送速率来减轻拥塞现象。该算法比较简单，可升级，但是对不同深度的结点有较大的影响，同时使用 ACK 也增加了额外开销。

7.3 传感网常用的操作系统

随着 WSN 网络应用复杂化，实时要求的提高，传统的前后台系统越来越不能适应系统发展，急需引入操作系统来减少软件开发难度、节约开发成本、提高效率。无线传感器网络操作系统（WSNOS）是 WSN 系统的基本软件环境，通过高效地利用无线传感器网络结点的有限资源为应用服务。

7.3.1 无线传感器网络特点及其对操作系统的特殊需求

在某种程度上可以将传感器网络看作一种有大量微型、廉价、能量有限的多功能传感器结点组成的，能协同工作的，面向分布式自组织网络的计算机系统。因此针对传感器网络应用的多样性、硬件功能有限、资源有限、结点微型化和分布式多协作等特点，研究和设计新的基于传感器网络的操作系统成为当前提高无线传感器网络性能的一个重要课题。目前，有些研究人员认为传感器网络的硬件很简单，没有必要设计一个专门的操作系统，可以直接在硬件上设计应用程序。这种观点在实际应用中会碰到很多问题。首先，面向传感器网络的应用开发难度会加大，应用开发人不得不直接面对硬件进行编程，无法得到像传统操作系统那样提供的丰富服务；其次，软件的重用性差，程序员无法继承已有的软件成果，降低了开发效率，增加研发成本。另一些设计人员认为，可以直接使用现有的嵌入式操作系统，Vxworks、WINCE、Linux、QNX 等。这些系统中有基于微内核架构的嵌入式操作系统，如 Vxworks、QNX 等，也有基于单体内核架构的嵌入式操作系统，如 Linux 等。由于这些操作系统主要面向嵌入式领域相对复杂的应用，其功能也比较复杂，如它们

可提供内存动态分配、虚拟内存实时性支持、文件系统支持等，但是系统代码尺寸相对较大。而传感器网络的硬件等资源极为有限，上述操作系统很难在无线传感器网络这样的硬件资源中高效运行。

由于传感器网络的特殊性，需要操作系统能够高效地使用传感器结点的有限内存、低功耗的处理器、传感器、低速通信设备、有限的电源等，且能够为各种特定应用提供最大的支持。在面向传感器网络的操作系统支持下，多个应用可以并发地使用系统资源，如计算、存储和通信等。在传感器网络中，传感器结点有两个突出的特点：①并发性很密集。它可能存在多个需要同时执行的逻辑控制，需要操作系统能够有效地满足这种发生频繁、并发程度高、执行过程比较短的逻辑控制流程。②传感器结点模块化程度很高。它要求操作系统能够让应用程序方便地对硬件进行控制，且在保证不影响整体开销的情况下，应用程序中的各个部分能够比较方便地进行重新组合。

7.3.2 TinyOS 开放源代码操作系统

TinyOS（TinyMicro Threading Operating System）是由加州大学伯克利分校开发的适应无线传感器网络的操作系统。TinyOS 操作系统库和应用程序都是用 NesC 编写的。NesC 是 C 语言的扩展，可用于开发组件化结构。其主要特点是：事件驱动模型、组件化编程、二级调度、轻量级任务、主动消息（AM）通信机制、分段操作（Spilt-phase Operations）。

（1）TinyOS 组件化结构

TinyOS 是由调度器和一系列组件组成。TinyOS2.x 体系结构如图 7-2 所示。其组件由下到上是：硬件抽象组件（hardware abstractions）、合成硬件组件（synthetic hardware）和高层软件组件（high level software）。硬件抽象组件负责物理硬件映射；合成硬件层实现不同数据格式的交互；高层软件组件负责数据处理、路由和传输等。在 TinyOS2.x 中，硬件抽象层 HAL 又分为三层，最底层为硬件表示层 HPL，中间层为硬件适配层 HAL，最顶层为硬件接口层 HIL。对于 TinyOSl.X 来说，这三层的引入不仅缓和了代码重用和移植问的矛盾，也提高了系统效率。

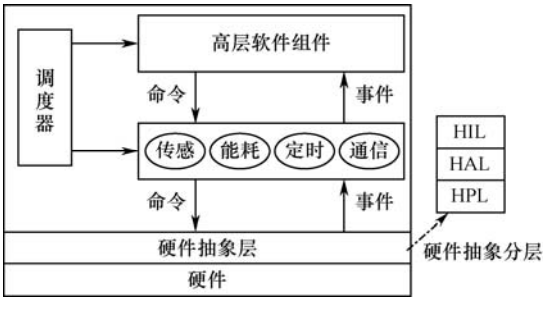


图 7-2　TinyOS2.x 体系结构

其中组件有：模块（module）和配置（configuration）。

每个组件由一系列命令和事件组成，这些命令和事件是组件相互联系的接口。上层组件向下层组件发出指令，下层组件向上层组件触发事件。组件模型先将多个不同组件组合到各层配置文件（configuration）中，再在应用程序的顶层配置文件中实现应用的整体装配。通过 ncc 编译器编译成 C 语言，再通过 gcc 编译器编译成单片机对应的目标代码。若组件稍有改动，需重新编译。

（2）TinyOS 调度机制

TinyOS 调度是任务和事件的二级调度。任务是单线程运行至完毕，不可相互抢占，但事件可抢占正在运行的任务或低优先级事件。任务用于实时要求不高的应用中，所有任务只分配单个任务栈，默认是简单的 FIFO 调度。若任务队列为空，CPU 进入休眠状态以降低功耗。其中任务默认数是 8 个，最大任务数是 255。还采用了分段操作来减少任务的运行时间，即分为程序启动硬件操作后迅速返回和硬件完成操作后通知程序两个阶段。

事件用于实时性有要求的应用中，可分为硬件事件和软件事件。硬件事件就是由底层硬件发出的中断，随后进入中断处理函数；软件事件则是带有 async 关键字的命令或事件函数，以通知相应组件做出适当的处理。在 TinyOS2.x 中，SchedulerBasicP 是主要的 TinyOS 调度器，提供带参数的 TaskBasic 接口。TinySchedulerC 是默认的调度器配件（configuration），可连接到 SchedulerBasicP。

（3）TinyOS 通信模型

TinyOS 的通信模型基于主动消息（Active Message），是一种高性能并行通信方式。在每次发送消息后，接收方需返回一个同步的确认消息。此确认消息是在主动消息层的最底层生成，其内容是一个特殊立即序列，发送方可迅速确定是否需重发消息。

在 TinyOSl.x 中，消息结构是 TOS_Msg，包含消息地址、消息类型、消息所属群号及消息处理函数 ID 等信息。在 TinyOS2.x 中，消息结构是 message_t，与 TOS_Msg 代表明确的主动消息数据包不同，message_t 兼容性更高，能使 data 域置于固定偏移位置，方便不同链路层间的通信。

当数据转发到无线传感器结点时，先存储在缓存中，然后由主动消息分发层交给上层应用组件对应的消息处理函数完以成消息的解包操作、计算处理或发送相应消息等工作。TinyOS 要求每个应用程序在消息被释放后能返回一块未用的消息缓存，以接收下一个未到的消息。TinyOS 通信的实现也是通过各层组件通信实现的，其结构如图 7-3 所示。

（4）能量管理

TinyOS2.X 使用了三种机制来管理和控制能量状态。

首先是 MCU 能量控制方式：dirty 标识位、低功耗状态计算函数 McuSleepC 和能量状态覆盖函数 PowerOverride。dirty 标识位通知 TinyOS 需计算一个新的低功耗模式。只要硬

件表示层组件对硬件配置进行了改动，MCU 的低功耗模式也会改变，就会调用 McuPower State.update()。接着调用 McuSleepC 计算出最佳低功耗模式，最后通过调用 Power Override. lowestState()以更新 MCU 功耗模式。

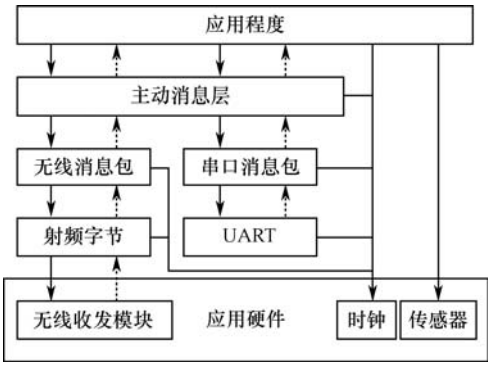


图 7-3　TinyOS 通信

每个设备都有个能量管理接口，即 StdControl 或 SplitControl 或 AsyncStd-Control。调用 stop 命令停止该设备，进入低功耗模式。

TinyOS 的定时器服务可以工作在大多数处理器的极低功耗的省电模式下。

7.4　传感网系统设计与分析

影响无线传感器网络系统设计的因素有很多，在设计时应遵循以下基本原则：

1）结点的小型化：在特殊场景应用中，特别是军事应用中，结点要求自身体积不能太大，主要是为了方便结点的部署，同时不易暴露。

2）结点适应性较强：监视目标区域的环境往往是十分恶劣、危险的，结点被部署到目标区域后，可以适应周围环境，并能进入工作状态。

3）网络的拓扑管理能力：由于多数结点布置在室外或环境条件比较恶劣的地方，对众多结点进行手动配置是比较困难的，所以要求系统能自动配置。所谓的配置，即在单个系统内，计算机、软件和硬件模块以及外部设备的一种特定的组合，它们互相连接起来以支持某种应用（系统）。此外，系统中有结点因能源耗尽或物理损伤而不能正常工作时，系统应能对新加入结点进行重新配置、重新组网，使系统继续正常工作。针对网络需求和任务的变化，系统会做出自动调节以适应这种变化。

4）数据路由：结点采集到数据后，可以及时、准确的传输到基站，这就要求数据的路

由可靠、路由时间短、结点的能耗低。

5）数据压缩处理：网络中由于传感器数量巨大、无线带宽有限，如果在传输过程中不对传输的数据进行必要的压缩，那么会造成网络通信的“拥塞”，甚至会使网络通信崩溃。为此有必要在数据传输时对数据进行压缩以减少通信的数据量，使得数据的实时性得到了进一步的保证。

6）鲁棒性：当一些传感器结点由于能源匾乏、物理损伤或外部环境干扰而出现故障和阻塞时，要求不会对整个传感器网络的检测任务产生影响，即系统所应具有的鲁棒性或容错性。鲁棒性需要进一步地模型化和定量化，鲁棒性和能源有效性之间存在着密切关系。在设计无线传感器网络系统时，需要权衡两者的利弊。

7）能源管理的有效利用：无线传感器结点完全脱离了导线连接，也就没有了外部的直接电源供应，而且针对布置在危险区域中的结点，对其所带电池进行更换是一项庞大的工作。所以针对结点的功耗和通信要求，需对能源进行智能管理和高效使用，使单个结点和整个网络系统尽可能长时间地保持正常工作。

8）系统成本：由于传感器是大批量地放置在目标区域，这样就造成单个传感器的制造成本决定了整个网络系统的造价。因此要尽可能的降低单个结点的成本。

7.5　典型系统设计与应用案例

7.5.1　在 ETC 系统中的应用

传感器网络在 ETC 系统中的应用实例如下。

ETC 又称电子收费系统，是 ITS 的重要组成部分。ETC 系统是一种能实现不停车收费的全天候智能型分布式计算机控制、处理系统，是电子技术、通信和计算机技术、自动控制技术、传感技术、交通工程和系统工程的综合产物，是典型的物联网应用。当车辆通过拥有 ETC 系统的收费站时，ETC 系统自动完成所过车辆的登记、建档、收费的整个过程，在不停车的情况下收集、传递、处理该汽车的各种信息。

基于 RFID 的不停车收费系统解决方案：ETC 的关键是利用在车载智能识别卡与收费站车辆自动识别系统的无线电收发器之间，通过无线电波进行数据交换，获取车辆的类型和所属用户等相关数据，并由计算机系统控制指挥车辆通行，其费用通过计算机网络从用户所在数据库申专用账号自动缴纳，如图 7-4 所示。

图 7-5 为某基于 RFID 技术的 ETC 系统车道示意图。ETC 车道主要由天线、地感线圈、自动栏杆、收费额显示牌、信号灯等组成。

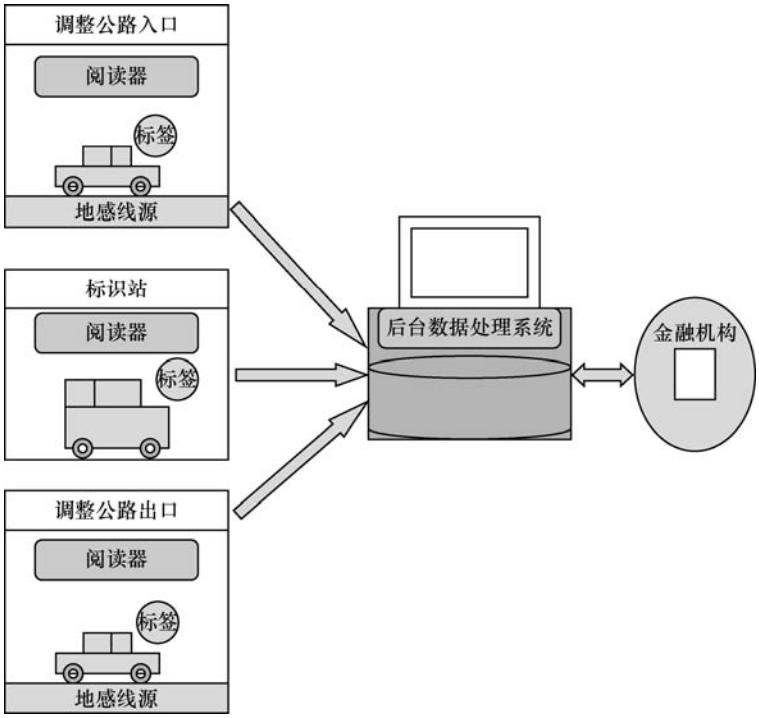


图 7-4　ETC 系统现场工作示意图

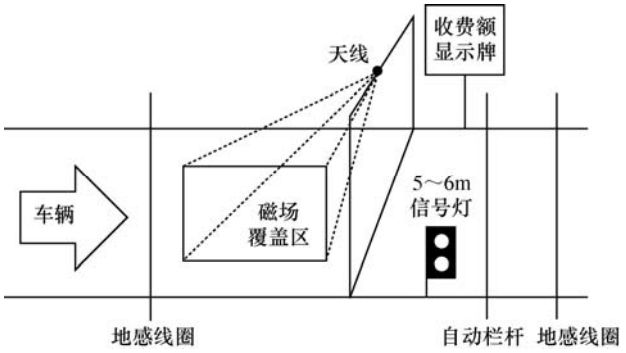


图 7-5　ETC 车道示意图

ETC 系统的工作流程为：

1）车辆进入通信范围时，首先压到地感线圈，启动天线。

2）天线与车载单元进行通信，判别车载单元是否有效。如有效，则进行交易；如无效（无效卡、无卡、假卡、低值卡等），则报警（通信信号灯变红）并保持车道关闭，进行人工收费。

3）如交易成功，系统控制栏杆抬升，通行信号灯变绿，收费额显示牌显示交易信息。

4）车辆通过落杆线圈后，栏杆自动回落，通信信号灯变红。

5）系统保持交易记录，并将交易信息上传至收费站服务器中，等待下一辆车进入。

整个 ETC 系统分为数据采集模块、数据传输模块、后台数据处理模块三个部分。

1）数据采集模块：采用 RFID 技术，主要由 RFID 车载超高频无源射频标签和电子读头设备、高速长距离超高频阅读器组成。RFID 可以采取非接触的射频通信方式，通过读写器与标签的无线通信实现数据采集，识别标签载体的身份特征等。

2）数据传输模块：以调整公路光纤网作为基础，无线网络为补充数据传输方案。

3）后台数据处理模块：负责基础数据的管理、系统安全管理、费用运算、路径运算、通行费拆分、系统相关报表管理等，以及与车载电子标签联名卡的办理、代扣通行费等金融方面的服务。

系统的三个模块组合在一起，形成一个完整的物联网，实现 ETC 功能。

将先进的信息技术、数据通信传输技术、电子控制技术以及计算机处理技术综合，有效地运用于公路运输管理系统，构成强大的交通物联网，将成为 21 世纪现代化运输体系的基本模式和发展方向，也是交通运输现代化的一个重要标志。

7.5.2　在水环境监测中的应用

太湖流域水环境信息共享平台采用物联网传感技术理念，运用先进的虚拟实境、视频监控、通信组网等信息化技术，按照“高标准、全覆盖、最先进”的要求，建设太湖流域水环境信息集成共享平台（见图 7-6）。平台建设覆盖流域内 282 家重点污染源、75 个水质自动站、53 个国家考核断面、21 个湖体监测点位和太湖蓝藻遥感预警监测，建成 50 个省、市、县和区域四级重点污染源监控中心，实现江苏省 742 家国、省控重点污染源自动监控设备与省厅监控中心 100%联网，实现涉太信息汇交共享，集成包括太湖流域水质自动监测、太湖蓝藻预警监测、重点污染源监测等十多个方面的信息和系统，承担流域范围内所有相关水环境监测、监控、预警和应急等信息集中处理分析任务。同时实现流域水环境全方位、一体化监控，在太湖流域水环境管理与决策中发挥了重要的支撑作用。通过这一涉及多系统、多部门的环境信息化工程建设，为探索将物联网应用于环境保护，建立环境信息资源共建共享，推进信息一体化建设做了有益的尝试与示范。

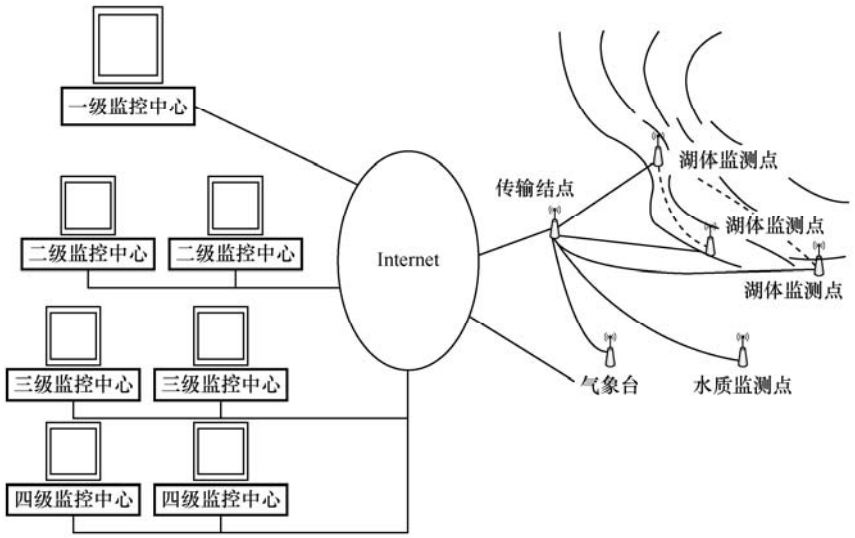


图 7-6　太湖流域水环境—物联网拓扑结构

在环境监测方面无锡市的“感知中国”物联网产业应用示范工程——“感知湖 • 智慧水利”是一个典型的代表。该示范项目是一套集防汛决策、水文监测、蓝藻治理、湖泛处置和水资源管理等诸多水利科技于一体的物联网决策指挥管理系统。在这个系统中安放有几百个球状浮标，它可用来进行对湖水上面的蓝藻进行检测。在这种浮球上面安装了一根杆，杆上安置了一块太阳能电池和工作芯片，为杆下的扩充系统进行供电。浮标下面的装置可以探测水里的蓝藻含量及其他参数。如果太湖水里的蓝藻含量一旦超标，芯片中的感应器就会通过无线网络向主控制台发出信号，控制台收到信号时就会立刻安排打捞船和工作人员前去打捞。“感知太湖 • 智慧水利”项目已经在无锡“感知中国”展厅里利用“模拟地球”演示物联网技术在水污染治理上应用的场景。传感技术使以往对太湖及人湖河道水质监测主要依靠人工巡视采样，费时费力且成效不高。现在使用物联网技术，通过在太湖水域内布放传感器和浮标搜集信息，再通过通信网络将搜集到的信息传到控制平台进行数据分析和处理，就可及时采集太湖水域的水质变化信息，洞悉各种污染源的排污情况，做到水文动态实时监控。大气环境污染衍生出温室效应、酸雨和臭氧层破坏。这种由环境污染衍生的环境效应具有滞后性，往往在污染发生当时不易被察觉或预料到，然而一旦发生就表示环境污染已经发展到相当严重的地步。

无线传感网对大气环境监测，是靠布设大量大气环境监测无线传感器，构成大气环境无线监测系统。通过微型传感器可以连续、自动采集大气的温度、气压、总可吸入颗粒物、CO_2、SO_2 和其他被监测气体参数。

7.5.3　在家庭监护中的应用

健康监测主要可用于人体的监护、生理参数的测量等，可以对人体的各种状况进行监控，并将数据传送到各种通信终端上。监控的对象不一定是病人，也可以是健康的人。各种传感器可以把测量数据通过无线方式传送到专用的监护仪器或者各种通信终端上，如PC、手机、PDA 等。我国目前已经进入了老龄化社会，下一代的健康与安全问题也日益引起人们关注，面向老人和儿童的个人健康监护需求将不继扩大。无线传感器网络将为健康控制提供更方便、更快捷的技术实现方法和途径，应用空间十分广阔。例如，在需要护理的中老年人身上，安装特殊用途传感器结点（如心率和血压监测设备），通过无线传感器网络，医生可以随时了解被监护病人的病情，进行及时处理，还可以应用无线传感器网络长时间地收集人的生理数据，这些数据在研制新药品的过程中是非常有用的。

加利福尼亚大学提出了基于无线传感器网络的人体健康监测平台 CustMed，以及可佩戴的传感器结点。结点采用加州大学伯克利分校研制、Crossbow 公司生产的 dot-mote，医生通过 PDA 可以方便、直观地查看人体的情况。

纽约 Stony Brook 大学针对当前社会老龄化的问题提出了监测老年人生理状况的无线传感器网络系统（Health Tracher 2000）。该系统除了监测用户的生理信息外，还可以在生命发生危险的情况下及时通报其身体情况和位置信息。结点采用了温度、脉搏、呼吸、血氧水平等多种类型的传感器。

美国南加州 VivoMetrics 健康信息与监测公司研制出嵌入无线传感器结点的“救生衬衫”。这种用于医疗和康复的衬衫穿在身上可以监测和记录血压、脉搏等 30 多种生理参数，并可以通过互联网发给医生。VivoMetrics 公司总裁 Paul Kennedy 说，救生衬衫可以读出你的每一次心跳和你情绪激动的状况，比如你的每一次叹息、每一次吞咽和每一次咳嗽。另外，纽约的 Sensatex 公司正在研制一种称作“智能衬衫”的产品。这种智能衬衫通过嵌入在布中的电光纤维收集生物医学的信息，可以监测心率、心电图、呼吸和血压等多种生理参数。运动员可用智能衬衫监测心率、呼吸和体温以提高训练成绩。甚至还能用它来听 MP3 音乐，麦克风也可以嵌入在衬衫里。消防队员可穿救生衬衫或智能衬衫监测烟吸入量，医生可用这种服装监测离开医院的患者。智能衬衫将收集到的信息传送到衬衫下面的发射器中，存储在芯片里或者通过无线网络发送给你的医生、教练或服务器。

7.5.4　在商城中的应用

物联网技术在商业和广场的客流管理和分析方面已得到广泛应用，如在一些商业经营场所出入口安装客流前端（摄像头和智能前端），通过有线或者无线方式接入客流分析管理平台。在营业时间内，客户进出商场，前端客流分析终端采集双向客流数据并传输到中心

平台。企业经营者通过计算机实时查看相应权限范围内的客流情况，掌握客流变化、分布情况，指导动态调整经营策略。尤其是商业连锁门店对客流分析与远程门店监控已成为基本配置手段，除在商业门店出入口安装摄像头对客流进行分析外，还在每个门店内部关键位置安装全球眼监控点用于视频监控。前端客流分析终端采集双向客流数据，传输到中心平台，重点区域视频通过视频服务器上传到全球眼平台。企业管理部门人员可通过 pc 实时掌握各个分店客流量变化以及对比分析经营情况，同时总部可实时监测各个分店关键位置视频画面。

上海“大悦城”是致力于创造未来购物体验的商城，不仅占据绝佳的地理位置与景观，更是吸纳新理念、新技术，倾心打造线上社区与线下体验，使得上海大悦城成为国内首家运用社会化媒体（Social Media）及物联网技术进行营销、运营的购物中心，将物联网技术融入到每个细节。首次进入购物中心，你只需及时取得上海大悦城的 VIP 会员资格即可尊享“大悦城城主”般的尊贵礼遇，在与三维现实空间平行的虚拟空间里，既有大悦城全心打造的基于社会化媒体和私有云计算的聚合应用平台及 RFID 远距离无源 VIP 会员卡，消费者们只需动动手指，不仅能与“姐妹淘”与“粉丝们”分享新鲜热辣的潮流娱乐新闻，还能第一时间在犹豫不绝时，听取远方挚友的购物建议，及时曝晒血拼战利品。更好的是消费者能私信大悦城的管理者，任何建言建议均能无障碍直达，享受“大悦城城主”般的尊贵礼遇。而轻松便捷的在线预订和餐饮排号服务，又能帮助消费者灵活管理个性化出行时间和消费行程，准备好随时邂逅商场里不可思议的精彩。最神奇的是，只需走入商场，在与现实平行的虚拟世界中，另一个“你”也化身为可爱的 3D 动画角色。在 RFID 物联网应用帮助下，它不仅能标记出你在现实商铺中的行动轨迹、消费足迹，还能参与最前卫的线上游戏，享受最酷炫的网络应用，并赢得限量版的纪念品。

随着生活水平的提高，人们从最初简单的购物发展到注重舒适及人性化需求。舒适、安全、便捷、时尚、尊贵已成为当今顾客的基本要求，以人为本的理念正被人们付诸实践。为了满足高端顾客的需求，建设具备物联网特征的智慧系统是目前及未来的必然趋势。运用物联网技术手段打造购物环境可以提高购物效率创造高额利润、提高服务水平提升客户满意度、增强企业竞争力吸引更多高端客户、提升企业信誉度塑造企业形象。

整个购物中心由于使用了智能化综合无线覆盖系统，消费者可以使用任意设备（计算机、手机、店内互动漫游终端）访问会员网络社区，浏览、评论（回复）、投票、分享（转发、收藏）时尚资讯和观点；利用现场视频直播系统坐在咖啡店里观看现场活动的精彩直播视频（在大型活动时更可以通过现场微博大屏幕实时参与现场互动）而不必亲临人头攒动的舞台现场；利用上海大悦城定制的手机应用上传街拍电子杂志，获取最新的商城/商户的店内活动（促销优惠、团购、超值抢购及特卖信息），通过到店参与和网络参与的双重方式享受个性化和差异化的推荐及折扣；同时，作为会员，消费者还可以轻松地在线管理自

己关注的品牌、好友及她们的收藏、购物行程、愿望和心得，使用自己的会员卡积分兑换功能与好友互赠礼物，通过“微博同城会”或发起或邀请或参与“美味「城」意”的店内主题活动，为自己赢得关注并因此获得积分。

（1）系统基本组成

该系统的基本组成是：布线系统、网络系统、RFID 标签应用（会员签到应用、餐饮叫号系统、手机应用）、RFID 信息采集、RFID 信息应用系统、现场视频直播系统、客流量统计分析系统、虚拟化云计算服务系统、中间件数据服务系统及后台管理系统。

1）客流量统计分析系统。

利用视频监控系统中的视频分析功能实现购物中心客流量统计，通过客流变化做出各种精确地客流分析。客流量直接影响销售额，通过客流分析，及时调整商品结构及管理思路，制定有效的市场推广活动策略，客观评估市场推广或促销活动成效，吸引更多的客户，进而提高销售额、完善管理流程、提高管理水平、提升行业竞争力。

2）系统结构与功能设计。

系统主要有如下功能：

- 商场的动线流量；
- 门店管理人员的管理水平考评；
- 商场的陈列、装修设计是否吸引人；
- 商场的黄金销售峰值与客流峰值；
- 促销活动带来的客流量和提袋率；
- 楼层/区域的客流量；
- 商场的营运管理；
- 销售成功率；
- 商场的推广活动效果；
- 什么时候是黄金销售时段；
- 销售人员的销售技巧；
- 购物广场客流量是否超出安全系数范围。

3）系统架构设计。

本系统采用的模式识别和计数算法，可对捕捉到的图像进行分析，准确区分人的大小特定影像，通过对人行走的动态轨迹综合分析处理，利用确认人的进出方向，实现客流量的统计。其原理是运用数字图像处理功能将模拟图像信息转换为数字图像信息，每隔 0.1 秒进行自动图像比较，通过运动趋势确定人的移动位置，从而获得多个目标的运动轨迹来确定通过人数。系统硬件基本构架如图 7-7 所示。

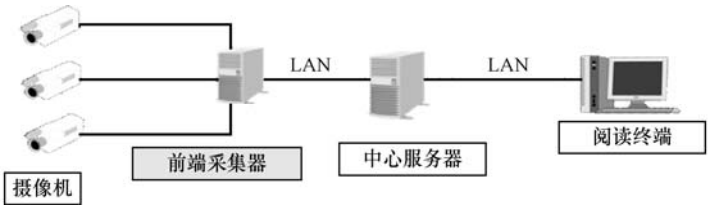


图 7-7　系统硬件构架

前端采用模拟摄像机，电源采用集中供电的方式；摄像机首先通过同轴电缆接入前端采集器，然后通过计算机网络系统与中心服务器进行连接；中心服务器安装客流量管理软件，并开发相应接口，供其他系统对其数据进行调取。

系统预设了感应范围，准确判断人的走向方向并避免徘徊等特殊情况的误算。

4）点位设计与安装：主要设置在商场主要出入口，餐厅出入口，活动现场出入口，重点关注区域出入口等。安装摄像机时，镜头与地面所成角度需要大于 80 度，以减少顾客在边沿位置时，客流统计的误差，提高准确度。可以根据客户的需要做不同的安装。系统可视功能基本配置示意如图 7-8 所示。

（2）扩展性和兼容性强的系统

1）后台系统可以兼容摄像机图像和热能图像分析；

2）可无缝连接客户 ERP 系统、MIS-POS 系统、CRM 会员系统，BI 数据挖掘系统；

3）对于连锁门店管理，没有数量限制。

（3）数据的准确性和完整性

1）数据唯一性：数据库数据唯一性；

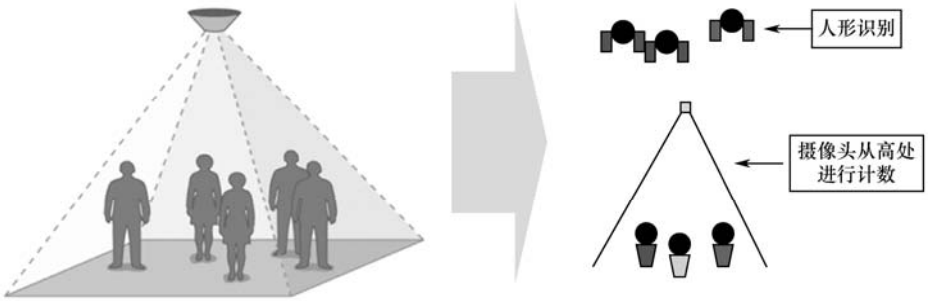


图 7-8　系统功能基本配置原理

2）数据准确性：90%以上的准确率；

3）数据完整性：系统有设立安全备份等功能，保证数据完整；

4）系统稳定性：长时间无故障工作。

（4）现场视频直播系统主要功能

可以通过现场微博大屏幕实时参与现场互动；

可通过 PC 平台（Windows/Linux/Mac OS X）上观看现场直播；

可通过手机平台（iPhone/Android/sybian/Windows Mobile）观看现场直播；

可通过购物中心内的各个信息显示屏直播。

1）系统组成与架构。

通过互联网将商场现场活动直播，对内通过综合信息发布系统将现场活动直播到各楼层的互动屏幕以及室外 LED 大屏幕，用户还可坐在咖啡店里观看现场活动的精彩直播。

前端视频直播固定摄像机通过网线连接到网络交换机，并通过交换机供电；现场移动机位则通过无线（Wi-Fi/3G）连接系统；所有信号再传输给数据服务器进行处理及管理并进行磁盘阵列存储。视频系统功能配置如图 7-9 所示。

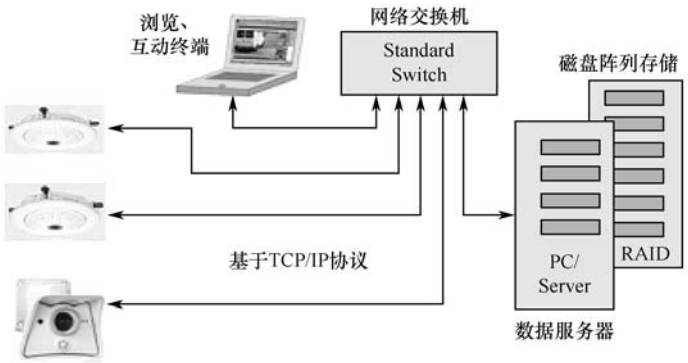


图 7-9　视频系统功能配置

2）基本要求。

高清视频：采用 360 度全景鱼眼、1/2 英寸的 CMOS 摄像机，独立的日/夜、远/近镜头，分辨率可以达到 320 万像素（2048×1536），超越 1080P 高清标准。

3）自适应码流。

通过二次编码支持多种不同的码流，对应不同的客户观看，例如：PC 用户可以观看超高分辨率的视频，同时如果手机用户浏览，系统会自动适应提供低分辨率的视频。

4）可伸缩性。

通过多服务器负载分担，系统能够支持几万用户在线观看。

（5）RFID 标签应用

该系统采用 RFID 被动式标签卡实现对大悦城会员管理功能，进一步通过对会员在大悦城中的消费行为进行统计分析，取得会员的消费习惯，再通对会员的个性化服务，实现

会员和商家的双赢的局面。RFID 应用子系统包括两个层面：一是 RFID 信息采集层面；二是通过对采集到的 RFID 信息进行统计分析，实现的应用系统。

1）系统 RFID 管理。

在系统中有大量的 RFID 使用，其管理系统的拓扑结构如图 7-10 所示。

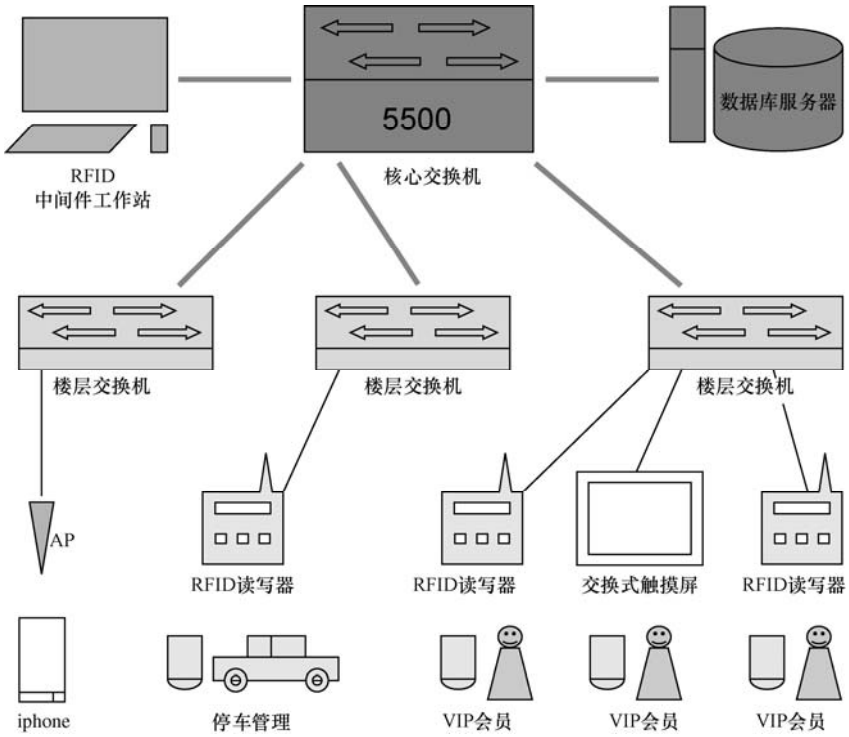


图 7-10　RFID 管理系统拓扑图

2）签到与查询应用。

商户签到：会员可利用分布在 B1－9F 的会员触摸屏终端或手机应用程序输入会员卡号及手机号后 4 位，进行“签到”。“签到”成功后，系统会自动回复短信，显示信息。

3）购物中心内餐饮及娱乐服务查询。

购物中心内餐饮及娱乐服务查询又名“懒人指南”或“约会地图”，根据会员现在的状态，给予商户推介信息，如“我已在购物中心内 XX 餐厅吃过饭”，手机系统给予相应推介“您可以接着逛 XX”商铺。如吃完午饭就推介游戏机或下午茶商户，吃完晚饭就推介电影院或甜品商户，类似此类的信息。

该应用基于一套会员消费与商户业态相结合的推介逻辑。目的是实现“吃、喝、玩、乐”的一站式消费指引。大的逻辑是基于业态的互补，细分的逻辑是基于会员的个性化特

征（如情侣逛街、同学逛街、同事逛街的选择，午饭目的、晚饭目的的选择等）。

4）商户优惠信息推送。

系统分为普通会员及 RFID VIP 会员，系统会自动为会员主动推送商户优惠信息。

基于 RFID 的信息采集与应用：RFID 的信息采集主要通过安装在大悦城各层的 RFID 读写器来实现。当会员身上携带 RFID 卡进入大悦城内时，其携带的 RFID 卡的信息就会被 RFID 读写器识别到，并立即通过网络记录到后台数据库中。系统记录的信息包括该 RFID 的 ID 号、行动轨迹、停留时间、位置等相关信息。

为了准确识别上述信息，在商城内需要的位置安装上一定数量 RFID 读写器，通过对建筑平面图和现场考察分析。如在 1 层的入口处配置 N 台读写器，各层需要的位置分别安装 N 台读写器，在超市入口处各配置 N 台读写器。凡是购买物品的顾客都通过 RFID 读写器结算。商城通过网络与后台相连，通过网络可实现所有读写器的管理。

5）RFID 信息应用系统。

通过采集到的 RFID 数据并进行统计分析，可获得如下信息：

- 门口会员流量统计：在大悦城入口安装的 RFID 读写器识别到会员的信息，通过网络传输到后台数据库，系统对这些信息进行统计分析，就能得相关流量信息。
- 门口会员偏好显示：系统通过识别进入大悦城的会员信息后，将会在大门口安装的交互式屏幕上，显示该会员及其好友感兴趣的信息，例如促销信息等。
- 交互式信息查询：当系统通过安装在各层的 RFID 读卡器识别到进入与其关联的交互式触摸屏附件时，在交互式屏幕上显示该楼层的促销信息、餐饮时间等重要提示信息。
- 会员消费信息统计分析：从会员进入大悦城起，其在大悦城内的行动轨迹、停留时间、消费信息等均能够被 RFID 系统采集到。并通过计算机网络记录到后台数据库，通过后台信息管理分析系统，能够统计分析出各种报表，供决策层参考。
- 其他推送信息：当会员在大悦城中被系统识别到时，其相关联的 iPhone 手机或其他终端将能够收到系统推送会员感兴趣的信息。

例如：当会员出现在影院门口时，将能够收到影院放映的影片信息等。

- VIP 停车服务：VIP 客户可以通过互联网或电话预约停车位及相关服务。

6）排队与叫号系统。

餐饮叫号系统是针对餐饮消费者排队时间过多与百货消费者不足的矛盾的一种解决方案。

- 会员通过会员社区及手机应用程序预定餐饮商户当天排队券。
- 会员到购物中心现场打票机输入会员卡号及手机号，打票机系统根据餐饮商户当前排队序列打印排队票据，同时，手机短信通知系统记录该票据编号。
- 当票据编号与排队序列距离 5 个号段时，手机短信通知系统向该会员发送短信通知。

7）与手机相连的应用。

手机应用基于会员社区网站后台，为智能手机用户提供掌上玩转大悦城的各项服务，功能包括：时尚博文、签到、懒人指南、视频直播、爱悦团、悦分享、影讯、微博、停车找位等。

8）虚拟化云计算服务系统。

上海大悦城物联网应用包括 RFID、流媒体应用、网站等多种应用，需要大量数据库服务器、文件服务器、WEB 服务器、流媒体服务器、POS 服务器、DNS 服务器、中间件服务器等。如果采用实体服务器，需要采购大量的服务器硬件、占据大量机房空间，而上海大悦城数据中心机房面积较小，而且预算有限，综合考虑各种情况，当采用 VMWare 虚拟化方案，通过虚拟化构建 IT 基础架构。系统组成的虚拟化服务平台建设包括 2 台实体 IBM 服务器、FC 光纤交换机、FC 磁盘整列、以太网和管理中心。2 台实体服务器配置 4 路 XEON 处理器、32G ECC 内存和 3 块 SAS 硬盘，安装 VMWARE ESX Server3.5 组成双机冗余热备。系统存储通过 FC 光纤交换机连接 FC 光纤通道磁盘整列，磁盘整列容量 36TB；虚拟机管理通过 VMWare Virtual Center 实现；虚拟化系统目前安装了 12 套虚拟机，包括数据库服务器、WEB 服务器、中间件服务器等。操作系统采用 Windows Server 2008 和 Red Hat Enterprise Linux5.5。构架如图 7-11 所示。

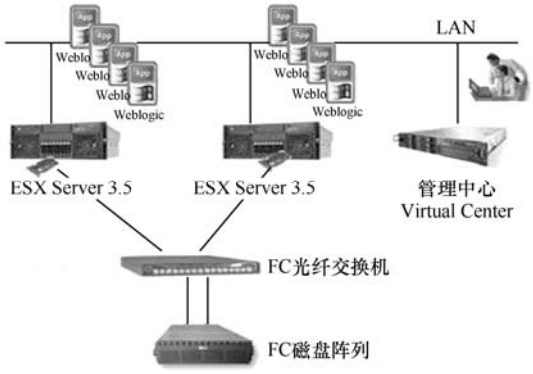


图 7-11　虚拟化云计算服务系统

9）中间件数据服务系统。

使用 BizTalk 构建了企业服务总线（ESB）。企业服务总线（ESB）可以提供通用的可重用服务，如协议转换、服务路由以及错误处理，同时可以提供数据透视功能，对于正在交互的应用程序数据内容进行监视。利用该项特性可以及时捕捉当前进入店中的 RFID 数据，根据 RFID 中的客户标示，实时地从会员管理系统及消费记录中获取会员历史记录，并且可以结合消费者行为分析系统的反馈结果，迅速在消费者附近的展示屏幕上发布有针对性的商品信息。

7.5.5　在机场安全系统中的应用

在机场周围安全防范方面，国内机场目前主要采用振动光纤、辐射电缆、红外对射、张力围栏、高压脉冲等“信号驱动”型技术手段，不可避免地存在漏警、误警现象。但是利用物联网就可以解决机场安全防范面临的各种问题。2009 年，无锡传感网中心的传感器产品在上海浦东国际机场和上海世博会被成功应用，首批价值 1500 万元的传感安全防护设备销售成功。该套设备采用一种“目标驱动”型安全防范技术，以 10 万个微小的传感器组成，这些传感器散布在墙头、墙角、墙面和周围道路上，构成强大的协同感知“物联网”，可实现全新的目标识别、多点融合和协同感知，对机场入侵目标进行有效分类和高精度区域定位，可防止人员的翻越、偷渡、恐怖袭击等攻击性人侵行为。

如 7-12 所示，浦东国际机场围栏外有一道无形的网，这个网由埋设在地下的传感器组成。这些传感器能够根据声音、图像、振动频率等信息分析判断爬上墙的究竟是人还是猫狗等动物，识别目标是什么，同时识别出物体的行为方式，比如说当物体接近栅栏时，系统能识别出是人还是车辆，是人在爬栅栏，还是风在吹栅栏，或是鸟停在栅栏上面晃动。不仅如此，系统还能够精确地进行定位，一旦发现有物体靠近栅栏，系统就会自动发出善意提醒——“机场禁区，请迅速离开，机场禁区，请迅速离开。”栏杆上的高音扬声器提醒来者迅速离开。如果来者不听警告，继续靠近栅栏，那么第二道防线就会报警。

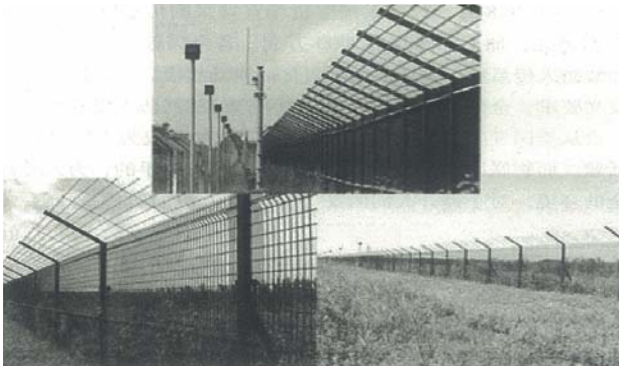


图 7-12　浦东国际机场围栏下布有传感器网

在铁栅栏里面，还有第三道电子传感围界，只要人员进入到机场的铁栅栏里面，报警系统也就相应提高到最高级别。这些传感器结点与机场控制大厅紧密相连。安全防范系统通过几个传感器的协同感知，确定来者位置，机场控制大厅里面的显示屏所对应的警务分片区就立刻变红闪烁，工作人员点击红色区域打开监控视频就能知道来者在做什么，进而采取行动。通过这些无形的传感网络，机场控制大厅就能够迅速对出现的报警情况进行处理。

由浦东国际机场在安防方面的投入不难看出，物联网在安防方面的需求潜力。浦东国

际机场在采购传感网产品方面仅一次采购就投入了 4000 多万元，加上配件共计 5000 多万元。若全国近 200 家民用机场都加装防入侵系统，则将产生上百亿的市场规模。国家民航总局正式发文要求，全国民用机场都要采用国产传感网防入侵系统。

在新一代传感器和物联网技术中，很多此类问题多采用电子围栏加以解决。

7.5.6 在电网故障诊断中的应用

智能电网在线监测及故障定位系统采用了数字化故障指示器和无线通信等技术，主要用于中高压输配电线路上，可检测和指示短路和接地故障，监测线路和变压器运行情况，对电动操作开关进行遥控、遥信（采集开关位置）操作。该系统可以帮助电力运行人员实时了解线路上各监测点的电流、电压、温度变化情况，在线路出现短路、接地、断线、绝缘下降等故障或者异常情况下给出声光或者短信通知报警，告如调度人员进行远程操作，以隔离故障和转移供电，通知电力运行人员迅速赶赴现场进行处理。

图 7-13 为某公司提供的在线监测及故障定位解决方案的系统结构。

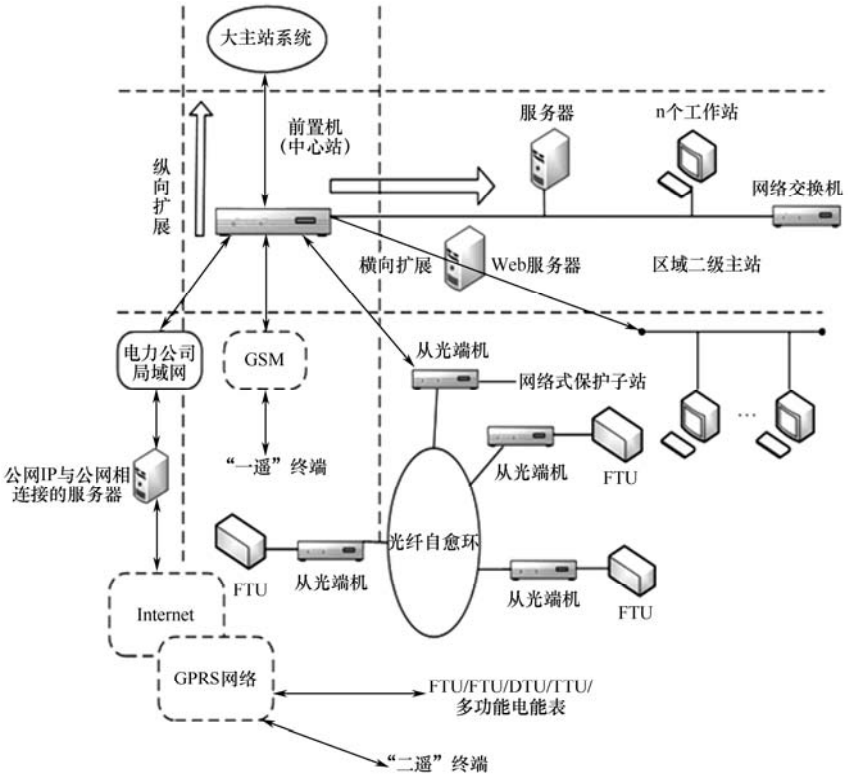


图 7-13　在线监测及故障定位系统结构

系统包括前置机（中心站）、Web 服务器、大主站系统及外设。

1）前置机（中心站）通过光纤、GSM 短信、GPRS 等与终端等通信，具有强大的数据处理功能和协议转换功能，是全系统的核心。

2）Web 服务器存储各种数据，这样就可以实现在网络上使用图形或表格等方式实时监测配电网运行情况和故障信息。

3）大主站系统是一个配电运行管理系统软件平台。系统从配电运行管理的业务流程出发，给用户提供了基于地理电网图、全网、单线图、厂站图、环网图、馈线图的配电运行管理功能，各种图形采用统一的图模库一体化设计，人机界面友好，使用简单方便，可实现数据共享，从而解决了运行调度与管理的图形差异带来的系统运行和维护问题。

前置机、Web 服务器、大主站系统及外设通过各种网络连接起来构成物联网，实现对电力系统在线监测及故障定位功能。

7.5.7　在制造系统中的应用

（1）在温/湿度方面的控制应用

温/湿度控制是通过有线宽带或 3G 无线网络，将各地的温/湿度信息上传到温/湿度数据增值服务平台，为客户提供即时温/湿度检测、即时报警、即时控制以及历史记录查询等服务。

此服务可为用户提供一个有效的节能管理手段，还可广泛用于急需温/湿度监控的养殖业、种植业、运输业、食品加工业等各行业。

该应用具有以下特点。

1）实时在线，统一的信息处理服务平台。可利用计算机、手机实时监控多个不同区域的数据、报警及控制信息。

2）低成本、高扩展性、免施工、易维护。

温/湿度控制可以应用于以下领域。

工业温/湿度监控。通过对温/湿度的监控可以判断生产设备的工作情况，从而使工作人员做出正确的判断和操作，因此温/湿度监控是工业生产自动化的重要方面。

农业温/湿度监控。农作物的生长，家禽的养殖以及农产品的保存等都与温/湿度密切相关。通过对温/湿度的监控可实时掌握生产情况，及时做出相应措施，保证农业生产的顺利进行。

其他行业温/湿度监控。温/湿度监控在安防、物流、能源等到众多领域均有其具体应用，创造了巨大的经济价值和社会价值。

（2）在电梯远程监测方面的应用

我国近年来始终保持高速增长，成为世界的大市场。车站、机场、商店、宾馆、住宅及商务楼，几乎任何较大的建筑物内都有电梯的身影。电梯给人们的工作、生活带来便捷，

但电梯带来的各种问题也影响了人们的工作和生活。图 7-14 所示为电梯监控系统示意图。

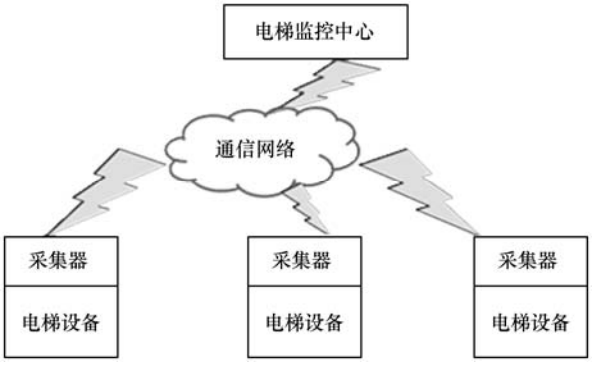


图 7-14　电梯监控系统示意图

1）核心需求。通过电梯维保关键技术研发，研究建立 3G 环境下电梯行业产品售后服务体系。系统依托电梯制造商已经建立的 PDM 系统、BI（商务智能）系统和 OA 办公自动化系统的集成和支持，通过先进的 3G 远程无线通信技术，实现电梯维保服务全过程信息化和智能化，为国内电梯行业向制造服务业的转型提供应用示范。

2）主要功能。电梯生产企业、电梯安装/维护企业、物业管理方可通过安装在电梯上的电梯监控装置，将电梯当前的设备型号、工作状态、性能参数、安装位置信息等数据通过无线网络（CDMA/GPRS）定时发送到电梯远程监控中心；监控中心工作人员可通过关键参数分析当前电梯的运行状态，通过对关键参数判断，在故障发生前即可察觉到故障预警，并根据电梯型号、安装位置等信息迅速准备好备品、备件，就近安排维护人员迅速赶赴现场，可大大降低设备故障率，提升售后服务响应速度，提高用户满意度。电梯远程监测系统的主要功能有电梯现场信息采集与管理、电梯维修管理、电梯保养管理、电梯安装管理、电梯产品信息管理和客户信息管理、电梯运行状况的统计、分析和预测。

7.5.8　在工业中的应用

油井远程监控应用通过提供油井现场的一体化生产数据及视频的采集、传输、监控，方便油田企业对生产现场进行实时监控，达到提高生产效率、节省成本的目的。图 7-15 为油田远程监控系统示意图。

1）核心需求。

采油井分布分散，多采用人工定时巡检、抽查的维护方式，一线工人劳动强度大，且由于人为因素难以保证资料录取的及时性和准确性，油井工作状况不能及时掌握，出现故障不能及时发现处理，因此希望借助信息化手段对采油设备安全生产进行监测与控制。

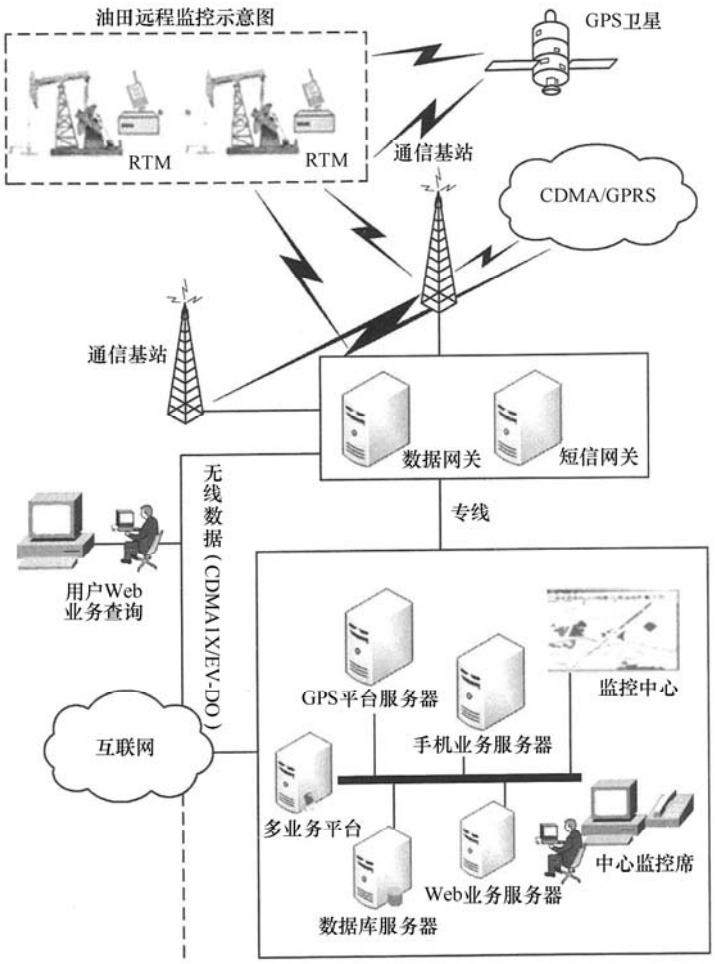


图 7-15　油田远程监控系统示意图

2）主要功能。

油井生产工况采集与监测：根据需要，在抽油机的不同部位安装相应的工作状态传感器及变送器，采集油井的生产参数，通过 CDMA 或 GPRS 网络把这些数据传送给后台应用系统，实现人工/自动远程控制。

故障诊断及报警功能：当发生停电、停机、回压异常、缺相及电流异常、抽油机抽空、曲柄销松脱等故障时，可以进行自动诊断并给出处理措施，实现工况诊断的智能化。

井场远程视频监控：对采油现场进行视频监控。

油井生产优化：通过对油井历史数据和当前数据，应用软件的数值仿真等功能，为油

井设计、油井生产、作业维护等进行参数调整，提供最优设计方案，减少损耗，提高效率。

（2）在输油管道监控方面的应用

输油管道监控应用是通过现场测量仪表测量输油管线压力、温度、流量、波势等参数，应用数据采集系统，通过无线或有线网络将数据传输至监控平台，建立一个管道运行实时监测系统，综合运用负压力波、流量在内的多种信号处理方法，能够及时准确地定位漏油点。

1）核心需求。近年来，社会上一些不法分子盗窃集输管线中的原油，原油泄漏事故频繁发生，造成了巨大的经济损失和环境污染，影响管道运行状况和环境安全；同时随着输油管道使用年限的不断增加，管道老化腐蚀泄漏对环境污染的问题越来越突出，所以需要建立一个能够及时发现泄漏并精确定位的监测系统。

2）主要功能。系统由数据采集分析、数据通信和数据监控处理三部分组成。

数据采集分析：包括放置在首端和末端的检测单元及数据采集控制、数据预处理装置。采集压力、流量和温度信号，对信号进行预处理后由通信装置送到数据监控处理装置。

数据通信：根据工况的不同，采用有线或无线传输的通信方式。无线方式包括 CDMA、GPRS 等数字通信。有线方式包括光缆、局域网络、有线电话及调制解调器等。

数据监控处理：中央数据处理计算、声光报警、运行参数及定位显示。

（3）在油罐车监控方面的应用

油罐车监控应用是指对油罐车的车辆运行监控和定位调度，实现实时监控车辆在路上的安全状况，对车辆危险情况做到实时监管。随时掌握所有车辆行驶及车辆装载情况，便于企业对车辆进行有针对性的调度，提高车辆的使用效率。

1）核心需求：保障车辆运行安全，提高运行效率。

2）主要功能。

视频监控：包括驾驶室和道路视频监控。

油罐监控：包括对油罐的温度、压力等的监控。

车辆调度：对所有车辆进行定位，随时了解车辆的行驶状况，并掌握所有车辆的分布情况，根据车辆分布情况，及时调整车辆运输线路。

对车辆行驶区域和线路进行监控，实现对车辆行驶区域的严格限制。

7.5.9 在远程医疗中的应用

远程医疗保健是通过体征仪表、数字化医疗设备、固定或移动网络、呼叫中心、网络平台等构成一套集预防、监测、定位、呼救于一体的远程健康救助服务体系。健康数据采集终端多种多样，健康 e 家系统的架构如图 7-16 所示。

传统的健康管理是在出现临床症状后，才去医院检查进行临床干预。统计数据显示，在健康阶段投入 1 元钱，就可以减少 8.59 元的医疗费用，还可以相应减少近百元的终末期抢救

费用，更重要的是病人少受罪，家人少受累，节约医疗费，造福全社会。生活节奏的加快，使得长期处于亚健康状态和患轻病的工作人群没有充分时间去医院治疗。对于这些人来说，如果能够做到随时随地连接医护资源，实现家庭保健自理，改善生活质量；做到日常检测、提示、咨询，就医建议，减少慢性病人病危情况；减少住院，降低综合医疗费用；在出现病症后可以方便地打通医院电话，进行预约或提前安排等，这势必会受到人们的欢迎。

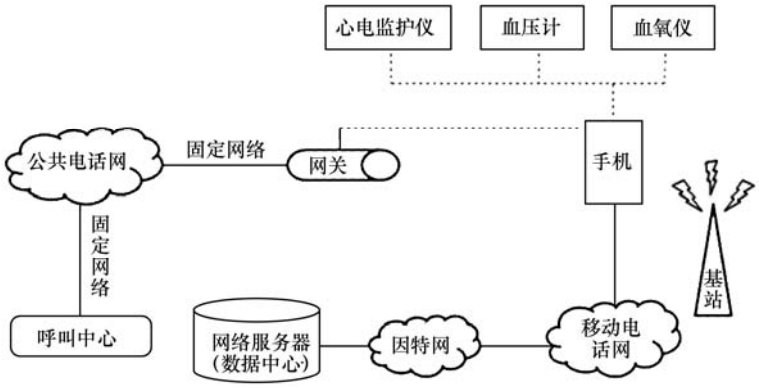


图 7-16　健康 e 家系统架构示意图

当前，医疗电子产品逐渐进入寻常家庭，大多使用方法简易，家用医疗器械的效果越来越显著，而且见效较快。这些都使得远程医疗健康保健进入家庭奠定了一定的基础。

远程医疗保健借助简易实用的家庭医疗传感设备，对家中病人或老人的生理指标进行自测，并将生成的生理指标数据通过固话网或 3G 无线网络传送到护理人或有关医疗单位，根据客户需求，还可提供相关增值业务，如紧急呼叫救助服务、专家咨询服务、终生健康档案管理服务等。远程医疗保健系统的主要功能包括以下几方面。

1）生命指征监测。

① 随时监测体温、脉搏、呼吸、血压、心电图、脑电图、血氧饱和度等关键生理指标。

② 测量数据自动或人工上传到电子病历中心，远端综合分析处理这些生理生化信号。

③ 通过移动、固定多种方式实现语音、数据的端到端交互。

2）健康评估。

① 测量数据以短信形式自动发给指定的亲属。

② 根据体检或健康指标采集终端，对健康情况进行评估。

③ 电子健康档案管理，可提供用户数据网站查询服务，每月出具健康管理分析报告。

④ 健康咨询：通过网络、手机，随时获得咨询、帮助，以及后续留诊挂号预约服务。

3）体征参数异常警告、一键呼救、健康关爱短信。用手机呼救时自动将室内/外位置发送给亲属及急救中心。